



## Cisco Aironet Wireless LAN Client Adapters Installation and Configuration Guide for MS-DOS

Corporate Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

Text Part Number: OL-1744-02

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCIP, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, Internet Quotient, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, IOS, IP/TV, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0203R)

*Cisco Aironet Wireless LAN Client Adapters Installation and Configuration Guide for MS-DOS*

Copyright © 2002, Cisco Systems, Inc.

All rights reserved.



## **Preface v**

Audience	vi
Purpose	vi
Organization	vi
Conventions	vi
Related Publications	vii
Obtaining Documentation	vii
World Wide Web	vii
Documentation CD-ROM	vii
Ordering Documentation	viii
Documentation Feedback	viii
Obtaining Technical Assistance	viii
Cisco.com	viii
Technical Assistance Center	ix
Contacting TAC by Using the Cisco TAC Website	ix
Contacting TAC by Telephone	ix

---

## **CHAPTER 1**

### **Overview 1-1**

Introduction to the Wireless LAN Adapters	1-2
Terminology	1-3
Parts of the Client Adapter	1-3
Radio	1-3
Radio Antenna	1-4
LEDs	1-4
Radio Ranges	1-4
Link Test	1-5
Data Transparency and Protocols	1-5
Protocols Supported	1-5
Security Features	1-6
System Configurations	1-6
Ad Hoc Wireless LAN	1-6
Wireless Infrastructure	1-7
Wireless Infrastructure with Workstations Accessing a Wired LAN	1-7
Extended Infrastructure Using Repeaters	1-8

Coverage Options 1-9  
     Minimal Overlap Coverage 1-9  
     Heavy Overlap Coverage 1-9  
     Multiple Overlapping Systems Coverage 1-10

CHAPTER 2

**Installing the Hardware 2-1**

Safety Information 2-2  
     FCC Safety Compliance Statement 2-2  
     Safety Guidelines 2-2  
     Warnings 2-2  
     Other Devices in the Wireless Network 2-3  
 Unpacking the Client Adapter 2-3  
     Package Contents 2-3  
     Antenna Connectors 2-4  
     Attaching a Remote Antenna 2-4  
     Detaching a Remote Antenna 2-5  
 Inserting the Client Adapter into a Computing Device 2-5  
     Inserting a PC Card 2-5  
     Inserting a PCI Client Adapter 2-6  
 Removing the Client Adapter 2-7  
     Removing a PC Card 2-7  
     Removing a PCI Client Adapter 2-7

CHAPTER 3

**Installing the Software 3-1**

Driver Overview 3-2  
 Windows for Workgroups 3.11 NDIS2 Installation 3-3  
 DOS NDIS2 Installation 3-3  
     DOS Packet Driver Installation 3-4  
 ODI Driver Installation 3-5  
 Additional Requirements and Features 3-5  
 Driver Keywords and Settings 3-6  
     Basic System Parameters 3-7  
     Network Performance Variables 3-8  
     Fragmentation Variables 3-9  
     Power Management Variables 3-10  
     Scanning Variables 3-12  
     Infrastructure Parameters 3-13  
     Ad Hoc Variables 3-16

## Adapter Keywords 3-16

## CHAPTER 4

**Utilities 4-1**

Site Survey and Link Test 4-2

Using Windows 3.11 or DOS to Perform a Link Test Using Telnet 4-2

Loading New Firmware Versions 4-3

DOS Utilities 4-3

Configuration Utilities 4-3

Diagnostic Utilities 4-4

DOS Utilities Running Environment 4-4

Layout and Format 4-4

General Usage Notes 4-5

Syntax 4-5

Running the Utilities 4-5

Getting Help 4-5

Configuration Utilities 4-6

AWCLEAP.EXE 4-6

AWCALLID.EXE 4-7

AWCALLID.EXE 4-8

WEPDOS.EXE 4-9

Diagnostic Utilities 4-10

PCMCIA.COM 4-10

RADINFO.EXE 4-11

## CHAPTER 5

**Error Messages and Trouble Shooting 5-1**

Accessing the Latest Troubleshooting Information 5-2

Interpreting the Indicator LEDs 5-2

If Your Radio Fails to Establish Contact 5-3

## APPENDIX A

**Technical Specifications A-1**

Technical Specifications A-2

## APPENDIX B

**Channels, Power Levels, Antenna Gains B-1**

Channel Sets B-2

Maximum Power Levels and Antenna Gains B-3

---

APPENDIX C

**Declarations of Conformity and Regulatory Information C-1**

- Manufacturers Federal Communication Commission Declaration of Conformity Statement C-2
  - Department of Communications – Canada C-3
    - Canadian Compliance Statement C-3
- European Community, Switzerland, Norway, Iceland, and Liechtenstein C-4
  - Declaration of Conformity with Regard to the R&TTE Directive 1999/5/EC C-4
- Declaration of Conformity for RF Exposure C-6
- Guidelines for Operating Cisco Aironet Wireless LAN Client Adapters in Japan C-7
  - Japanese Translation C-7
  - English Translation C-7

---

APPENDIX D

**Translated Safety Warnings D-1**

- Explosive Device Proximity Warning D-2
- Lightning Activity Warning D-3
- Installation Warning D-3
- Circuit Breaker (15A) Warning D-4

---

INDEX



## Preface

---

This preface provides an overview of the *Cisco Aironet Wireless LAN Client Adapters Installation and Configuration Guide for MS-DOS*, references related publications, and explains how to obtain other documentation and technical assistance, if necessary.

These topics are covered in this section:

- Audience, page vi
- Purpose, page vi
- Organization, page vi
- Conventions, page vi
- Related Publications, page vii
- Obtaining Documentation, page vii
- Obtaining Technical Assistance, page viii

# Audience

This publication is for the person responsible for installing, maintaining, and configuring a Cisco Aironet Wireless LAN Adapter (also referred to as an *adapter* or *client adapter*) on a computer using the MS-DOS operating system. The installer should be familiar with MS-DOS, computing devices and with network terms and concepts.

# Purpose

This publication describes the adapters, explains how to install the adapters and the associated drivers and software, and offers troubleshooting information.

# Organization

Please read Chapters 2 and 3 before attempting to install or use the hardware and software described in this guide.

This guide is arranged as follows:

Chapter 1, “Overview,” provides you with a general introduction to the wireless LAN adapters, describes direct sequence radio technology, and the various adapter configurations you can use when operating the adapter in your infrastructure.

Chapter 2, “Installing the Hardware,” describes the physical installation of the adapter and the standard antenna.

Chapter 3, “Installing the Software,” describes the installation and configuration of the various network drivers.

Chapter 4, “Utilities,” provides detailed procedures for using the utilities to perform link tests, site surveys, configuration, diagnostics, as well as loading new firmware versions.

Chapter 5, “Error Messages and Trouble Shooting,” provides detailed descriptions of the LED messages and error codes, as well as general procedures for correcting common problems.

Appendix A, “Technical Specifications,” provides radio and physical specifications.

Appendix B, “Channels, Power Levels, Antenna Gains,” provides channel identifiers and channel center frequencies for various area regulatory agencies.

Appendix C, “Declarations of Conformity and Regulatory Information,” provides conformity information about the adapter.

# Conventions

This publication uses the following conventions to convey instructions and information:

- Commands and keywords are **boldface**.
- Variables are in *italics*.
- Notes, cautions, and warnings use the following conventions and symbols:



**Note**

Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.

**Caution**

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

## Related Publications

For more information about Cisco Aironet Wireless LAN Adapters and related products, refer to these publications:

- *Quick Start Guide for Cisco Aironet Wireless LAN Client Adapters*
- *Release Notes for Cisco Aironet Wireless LAN Client Adapters*
- *Quick Start Guide: Cisco Aironet Access Points*
- *Cisco Aironet Access Point Hardware Installation Guide*
- *Cisco Aironet Access Point Software Configuration Guide*
- *Cisco Aironet Wireless LAN Client Adapters Installation and Configuration Guide for Linux*
- *User's Guide and Technical Reference Manual Aironet Wireless LAN Adapter PC4500 and PC4800*

## Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

### World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- <http://www.cisco.com>
- <http://www-china.cisco.com>
- <http://www-europe.cisco.com>

### Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and might be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

## Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:  
[http://www.cisco.com/cgi-bin/order/order\\_root.pl](http://www.cisco.com/cgi-bin/order/order_root.pl)
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:  
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408-526-7208 or, in North America, by calling 800-553-NETS(6387).

## Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Attn Document Resource Connection  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate your comments.

## Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

## Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

<http://www.cisco.com>

## Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

### Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

<http://www.cisco.com/tac>

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

<http://www.cisco.com/register/>

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

<http://www.cisco.com/tac/caseopen>

### Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.





## Overview

---

This chapter describes the Cisco Aironet Wireless LAN Client Adapter, also referred to as an *adapter* or *client adapter*, and illustrates its role in a wireless network.

These topics are covered in this section:

- Introduction to the Wireless LAN Adapters, page 1-2
- Parts of the Client Adapter, page 1-3
- Radio Ranges, page 1-4
- Data Transparency and Protocols, page 1-5
- System Configurations, page 1-6
- Coverage Options, page 1-9

# Introduction to the Wireless LAN Adapters

The Cisco Aironet Wireless LAN Client Adapters, also referred to as *adapters*, are radio modules that provide transparent, wireless, data communications between fixed, portable, or mobile devices and other wireless devices or a wired network infrastructure. The adapters are fully compatible when used in devices supporting Plug-and-Play (PnP) technology. Host devices can be any device equipped with a PC Card Type II or Type III slot. These devices include:

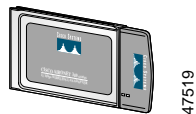
- Desktop systems
- Portable laptops
- Notebook computers
- Personal digital assistants
- Pen based computers
- Other data collection devices

The primary function of the adapters is to transfer data packets transparently through the wireless infrastructure. The adapters operate similarly to a standard network product except that the cable is replaced with a radio connection. No special wireless networking functions are required, and all existing applications that operate over a network can operate using the adapters.

The PC Card can also be built into peripheral devices such as printers to provide them with a transparent wireless connection to a wired network.

This document covers three types of adapters:

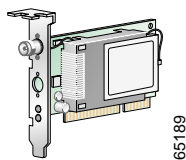
- PC card client adapter (also referred to as a *PC card*)—A PCMCIA card radio module that can be inserted into any device equipped with an *external* Type II or Type III PC card slot. Host devices can include laptops, notebook computers, personal digital assistants, and hand-held or portable devices.



- LM card client adapter (also referred to as an *LM card*)—A PCMCIA card radio module that can be inserted into any device equipped with an *internal* Type II or Type III PC card slot. Host devices usually include hand-held or portable devices.



- PCI client adapter—A client adapter card radio module that can be inserted into any device equipped with an empty PCI expansion slot, such as a desktop computer.



Refer to the “Radio Antenna” section on page 1-4 for antenna differences between these adapters.

## Terminology

Throughout this document, these terms are used:

- client adapter—Refers to all three types of adapters
- PC card, LM card, or PCI client adapter—Refers only to a specific adapter
- workstation (or **station**)—Refers to a computing device with an installed client adapter
- End Node—A client node that is located at the end of the Network Tree.
- Infrastructure—The wireless infrastructure is the communications system that combines access points, mobile nodes, and fixed nodes. Access points within the infrastructure can be either root units, which are physically wired to the LAN backbone, or can act as wireless repeaters. Other RF enabled devices serve as fixed nodes or mobile client nodes.
- Parent/Child Node—Refers to the relationships between nodes in the wireless infrastructure. The complete set of relationships is sometimes described as a network tree. For example, the access point (at the top of the tree) would be the parent of the end nodes. Conversely, the end nodes would be the children of the access point.
- Power Saving Protocol (PSP) and Non-Power Saving Protocol—The Power Saving Protocol allows computers (usually portable computers) to power up only part of the time to conserve energy. If a client node is using the Power Saving Protocol to communicate with the network, the access point must be aware of this mode and implement additional features such as message store and forward. If the client node is powered from an AC line, do not use PSP.
- Repeater—A repeater is an access point that extends the radio range of the infrastructure. A repeater is not physically attached to the wired LAN, but communicates through radio to another access point, which is either a root unit or another repeater.
- Root Unit—The root unit is an access point that is located at the top, or starting point, of a wireless infrastructure. A root unit provides the physical connection to the wired LAN and contains configuration information in its association table that covers all nodes that access the wired network (backbone). All access points directly attached to the wired LAN backbone are root units.

## Parts of the Client Adapter

The client adapter is composed of three major parts: a radio, a radio antenna, and two LEDs.

### Radio

The client adapter contains a direct-sequence spread spectrum (DSSS) radio that operates in the 2.4-GHz license-free Industrial Scientific Medical (ISM) band. The radio transmits data over a half-duplex radio channel operating at up to 11 Mbps.

DSSS technology causes radio signals to be transmitted over a wide frequency range, using multiple frequencies simultaneously. The benefit of this technology is its ability to protect the data transmission from interference. For example, if a particular frequency encounters noise, interference, or both, enough redundancy is built into the signal on other frequencies that the client adapter usually is successful in its transmission.

## Radio Antenna

The type of antenna used depends on your client adapter:

- PC cards have an integrated, permanently attached diversity antenna. The benefit of the diversity antenna system is improved coverage. The system works by allowing the card to switch and sample between its two antenna ports in order to select the optimum port for receiving data packets. As a result, the card has a better chance of maintaining the radio frequency (RF) connection in areas of interference. The antenna is located within the section of the card that protrudes from the PC card slot when the card is installed.
- LM cards are shipped without an antenna; however, an antenna can be connected through the card's external connector. If a snap-on antenna is used, it should be operated in diversity mode. Otherwise, the antenna mode used should correspond to the antenna port to which the antenna is connected.
- PCI client adapters are shipped with a 2-dBi dipole antenna that attaches to the adapter's antenna connector. However, other types of antennas can be used. PCI adapters can be operated only through the antenna port located on the right side of the radio module (not to be confused with the antenna connector on the card carrier).



### Note

---

External antennas used in combination with a power setting resulting in a radiated power level above 100 mW equivalent isotropic radiated power (EIRP) are not allowed for use within the European community and other countries that have adopted the European R&TTE directive. CEPT recommendation Rec 70.03, or both. For more details on legal combinations of power levels and antennas in those countries, contact Cisco Corporate Compliance.

---

## LEDs

The adapter has two LEDs that glow or blink to show the status of the adapter or to convey error messages. See “Interpreting the Indicator LEDs” section on page 5-2 for an interpretation of the LED codes.

## Radio Ranges

Because of differences in component configuration, placement, and physical environment, every network application is a unique installation. Before installing the system, you should perform a site survey in order to determine the optimum utilization of networking components and to maximize range, coverage, and network performance.

Here are some operating and environmental conditions that you need to consider:

- **Data Rates**—Sensitivity and range are inversely proportional to data bit rates. The maximum radio range is achieved at the lowest workable data rate. There is a decrease in receiver threshold sensitivity as the radio data rate increases.
- **Antenna Type and Placement**—Proper antenna configuration is a critical factor in maximizing radio range. As a general guide, range increases in proportion to antenna height.



**Note**

For a detailed explanation of antenna types and configurations along with guidelines on selecting antennas for specific environments, see the *Aironet Antenna Guide* on Cisco's web site:

[http://www.cisco.com/univercd/cc/td/doc/product/wireless/air\\_legc/antennas/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/wireless/air_legc/antennas/index.htm)

- **Physical Environments**—Clear or open areas provide better radio range than closed or filled areas. Also, the less cluttered the work environment, the greater the range.
- **Obstructions**—Avoid locating the computing device and antenna in a location where there is a metal barrier between the sending and receiving antennas.
- **Building Materials**—Radio penetration is greatly influenced by the building material used in construction. For example, drywall construction allows greater range than concrete blocks. Metal or steel construction is a barrier to radio signals.

## Link Test

The link test tool is used to determine RF coverage. The test results help the installer eliminate low RF signal level area that can result in loss of connection.

**Note**

External antennas used in combination with a power setting resulting in a radiated power level above 100 mW equivalent isotropic radiated power (EIRP) are not allowed for use within the European community and other countries that have adopted the European R&TTE directive or the CEPT recommendation Rec 70.03 or both. For more details on legal combinations of power levels and antennas in those countries, contact Cisco Corporate Compliance.

## Data Transparency and Protocols

The Cisco Aironet Wireless LAN Adapter transports data packets transparently as they move through the wireless infrastructure. The PC Card operates similarly to a standard network product except that the wire is replaced with a radio connection. No special wireless networking functions are required. All existing applications, which operate over a network, operate using the Cisco Aironet Wireless LAN Adapter.

## Protocols Supported

The Cisco Aironet Wireless LAN Client Adapter can be used in a variety of infrastructure configurations. Cisco Aironet access points provide connections to Ethernet Networks. When using the Cisco Aironet standard device drivers, the PC Card is fully compliant with the protocols and wired networks listed in Table 1-1

**Table 1-1** *Protocols Supported*

Drivers	Operating Systems
ODI	MS-DOS-based driver for Novell NetWare

Table 1-1 Protocols Supported

Drivers	Operating Systems
NDIS2	MS-DOS, Windows 3.xx
Packet	MS-DOS, Windows 3.xx

## Security Features

The Cisco Aironet Wireless LAN Client Adapter employs Direct Sequence Spread Spectrum Technology, previously developed for military *anti-jamming* and *low probability of intercept* radio systems.

The access point must be set to the same SSID as all other devices on the wireless infrastructure. Units with a different SSID cannot directly communicate with each other.

## System Configurations

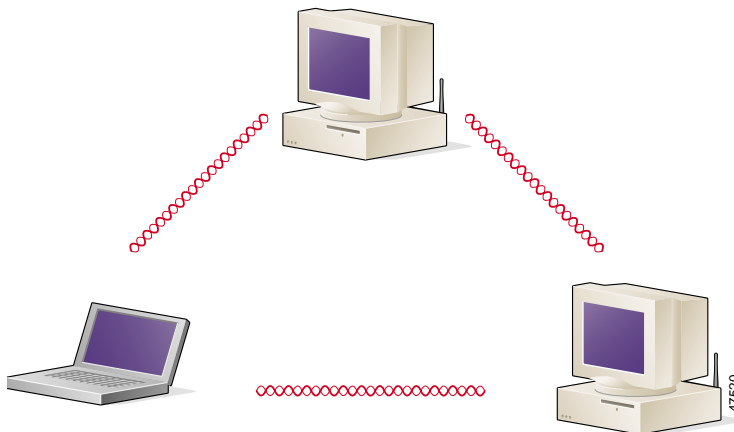
The Cisco Aironet Wireless LAN Client Adapter can be used in a variety of network system configurations. Access points provide connections to your Ethernet networks or act as repeaters increasing wireless communication range. The maximum communication range is based on how you configure your wireless infrastructure.

Examples of some common system configurations are shown on the pages that follow, along with a description of each.

## Ad Hoc Wireless LAN

An ad hoc wireless LAN (Figure 1-1) is the simplest wireless LAN configuration. In a wireless LAN, using an ad hoc network operating system (such as Windows for Workgroups), all devices equipped with the PC Card can be linked together and communicate directly with each other

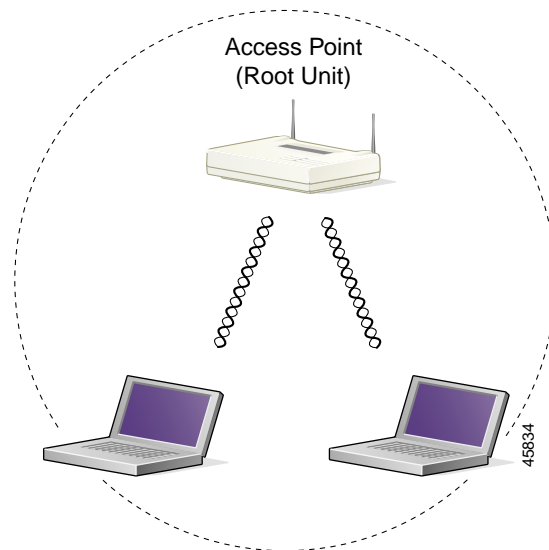
Figure 1-1 Ad Hoc Wireless LAN



## Wireless Infrastructure

In a wireless infrastructure (Figure 1-2), an access point is used as a stand alone root unit. The root unit is not attached to any wired LAN (such as an Ethernet LAN), but functions as a hub linking all stations together. This configuration is similar to the ad hoc network, except that the access point serves as the focal point for communications. This increases the effective communication range over the ad hoc LAN because both stations are not required to be in direct communication range of each other.

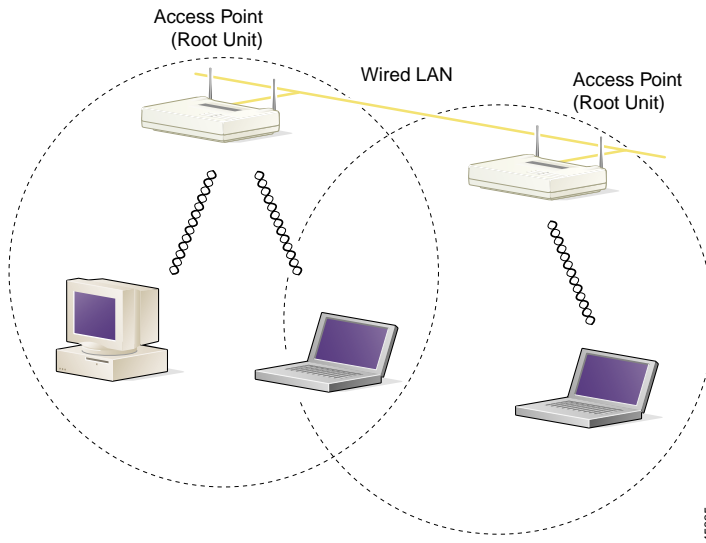
**Figure 1-2** *Wireless Infrastructure*



## Wireless Infrastructure with Workstations Accessing a Wired LAN

A micro-cellular network can be created by placing two or more access points on a LAN (Figure 1-3). The roaming protocols allow remote workstations to move from one microcell domain to another. The process is seamless and transparent. The connection to the file server or host is maintained without disruption. This configuration is useful with portable or mobile stations, allowing them to be directly connected to the wired network even while moving about (roaming). When an infrastructure is configured by using multiple access points and repeaters, a mobile station is automatically associated and re-associated to the access point which provides the best performance. This is referred to as seamless roaming.

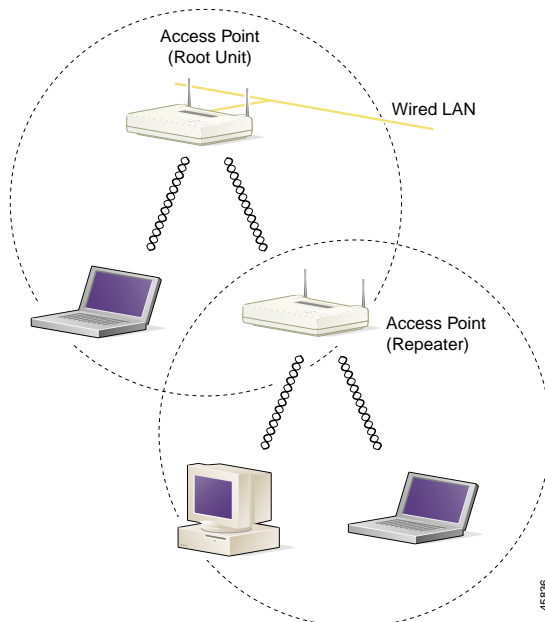
**Figure 1-3** *Wireless Infrastructure with Workstations Accessing a Wired LAN*



## Extended Infrastructure Using Repeaters

An access point can be configured as a stand-alone repeater to extend the range of your infrastructure, or to overcome an RF blocking obstacle (Figure 1-4). The repeater forwards traffic between the Cisco Aironet Wireless LAN Client Adapter equipped workstations and devices and the wired LAN by sending packets to either another repeater or to another access point attached to the wired LAN. The data is sent through whichever route provides the greatest performance for the client. Multiple repeater hops can be supported in the path to the wired LAN.

**Figure 1-4** *Extended Infrastructure Using Repeaters*



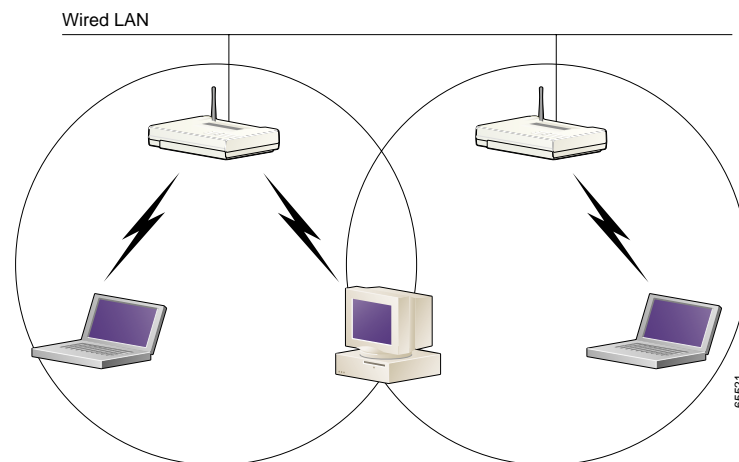
# Coverage Options

The system architecture options of the wireless station and access points provide for a variety of coverage alternatives and flexibility. The system can be designed to provide a wide coverage area with minimal overlap (Figure 1-5) or coverage with heavy overlap (Figure 1-6). The latter improves system performance and protection against downtime in the event of a component failure.

## Minimal Overlap Coverage

By arranging the access points so that the overlap in coverage area is minimized, a large area can be covered with minimal system cost (Figure 1-5). The total bandwidth available to each mobile station depends on the amount of data each mobile station needs to transfer and the number of stations located in each cell. Seamless roaming is supported as a mobile station moves in and out of range of each access point, thereby maintaining a constant connection to the wired LAN. Each access point (and adapter) must be configured with the same SSID to provide the roaming capability.

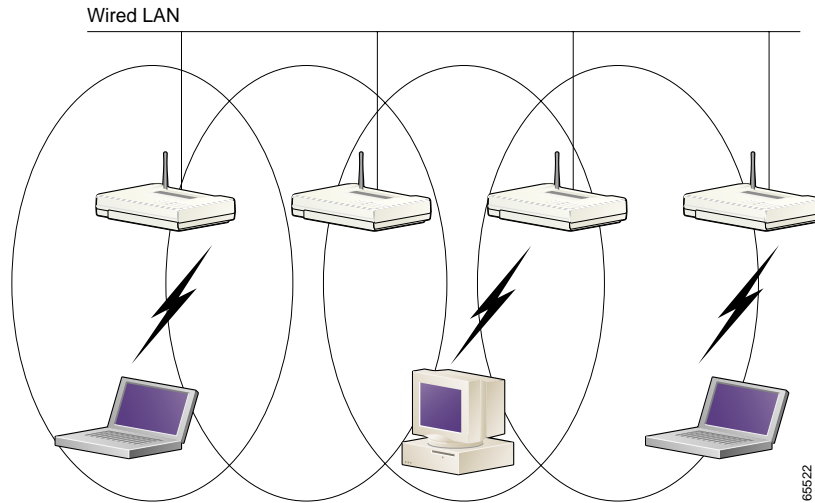
**Figure 1-5 Minimal Overlap Coverage Option**



## Heavy Overlap Coverage

By arranging the access points so that the overlap in coverage area is nearly maximized, a large number of mobile stations can be supported in the same wireless infrastructure (Figure 1-6). However, units in overlapping coverage areas on the same frequency will detect adjacent cell traffic and delay transmissions that would cause collisions. This reduces the aggregate radio system throughput. Heavy cell overlap is not recommended for maximum system throughput. Due to the redundancy in coverage overlap, system access is not lost if an access point fails. If the access point fails, the station automatically roams to an operational access point. With this system architecture, all access points and PC Card units must be configured with the same SSID.

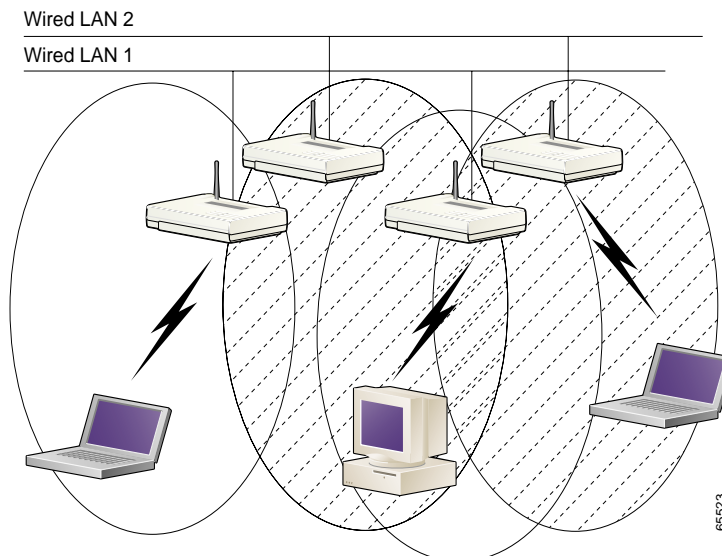
**Figure 1-6 Heavy Overlap Coverage Option**



## Multiple Overlapping Systems Coverage

Multiple systems can operate in the same vicinity (Figure 1-7). The architecture provides multiple channels, which can exist in the same area with virtually no interference to each other. In this mode, each system must be configured with different SSIDs and different channels, which prevent clients from roaming to access points of a different wireless system.

**Figure 1-7 Multiple Overlapping Systems Coverage Option**





## Installing the Hardware

---

This section describes the procedures for installing the Cisco Aironet Wireless LAN Client Adapter.

These topics are covered in this section:

- Safety Information, page 2-2
- Unpacking the Client Adapter, page 2-3
- Inserting the Client Adapter into a Computing Device, page 2-5
- Removing the Client Adapter, page 2-7

# Safety Information

Follow the guidelines in this section to ensure proper operation and safe use of the client adapter.

## FCC Safety Compliance Statement

The FCC, with its action in ET Docket 96-8, has adopted a safety standard for human exposure to RF electromagnetic energy emitted by FCC-certified equipment. Cisco Aironet products meet the uncontrolled environmental limits found in OET-65 and ANSI C95.1, 1991. Proper operation of this radio device according to the instructions in this publication will result in user exposure substantially below the FCC recommended limits.

## Safety Guidelines

- Do not touch or move the antenna while the unit is transmitting or receiving.
- Do not hold any component containing a radio such that the antenna is very close to or touching any exposed parts of the body, especially the face or eyes, while transmitting.
- Do not operate the radio or attempt to transmit data unless the antenna is connected; otherwise, the radio can be damaged.
- Use in specific environments:
  - The use of wireless devices in hazardous locations is limited to the constraints posed by the safety directors of such environments.
  - The use of wireless devices on airplanes is governed by the Federal Aviation Administration (FAA).
  - The use of wireless devices in hospitals is restricted to the limits set forth by each hospital.
- Antenna use:
  - To comply with FCC RF exposure limits, dipole antennas should be located at a minimum distance of 7.9 inches (20 cm) or more from the body of all persons.
  - High-gain, wall-mount, or mast-mount antennas are designed to be professionally installed and should be located at a minimum distance of 12 inches (30 cm) or more from the body of all persons. Please contact your professional installer, VAR, or antenna manufacturer for proper installation requirements.

## Warnings

Observe the following warnings when operating the client adapter:



Warning

---

**Do not operate your wireless network device near unshielded blasting caps or in an explosive environment unless the device has been modified to be especially qualified for such use.**

---



**Warning**

---

In order to comply with RF exposure limits established in the ANSI C95.1 standards, it is recommended when using a laptop with a PC card client adapter that the adapter's integrated antenna is positioned more than 2 inches (5 cm) from your body or nearby persons during extended periods of transmitting or operating time. If the antenna is positioned less than 2 inches (5 cm) from the user, it is recommended that the user limit exposure time.

---

Translated versions of these safety warnings are provided in Appendix D.

## Other Devices in the Wireless Network

Refer to the user's guide and technical reference manual for the access point, universal client, or bridge for additional information.

## Unpacking the Client Adapter

Follow these steps to unpack the client adapter:

- 
- Step 1** Open the shipping container, and carefully remove the contents.
- Step 2** Return all packing materials to the shipping container, and save it.
- Step 3** Ensure that all items listed in the "Package Contents" section are included in the shipment. Check each item for damage.

**Note**

---

If any item is damaged or missing, notify your authorized Cisco sales representative. Any remote antenna and its associated wiring are shipped separately.

---

## Package Contents

Each client adapter is shipped with the following items:

- Cisco Aironet PC Card Client Adapter, Cisco Aironet LM Card Client Adapter, or Cisco Aironet PCI Client Adapter
- 2-dBi dipole antenna (for PCI client adapter)
- *Quick Start Guide: Cisco Aironet Wireless LAN Client Adapters*
- Cisco Aironet Series Wireless LAN Client Adapters Drivers and Utilities CD
- Cisco product registration card

**Note**

---

The MS-DOS drivers and utilities are not shipped with the adapter. Follow this path to download them from Cisco.com: **Service & Support > Technical Assistance Center > Software Center > Wireless Software**.

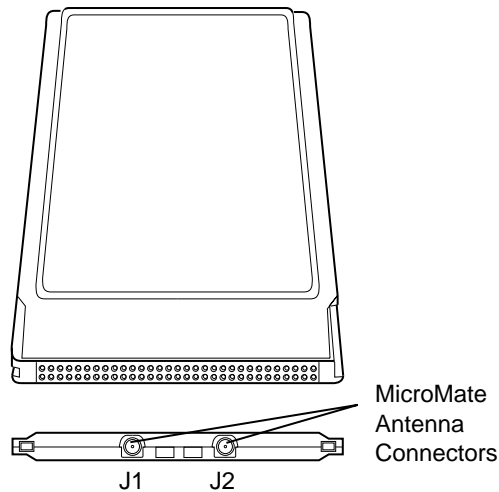
---

## Antenna Connectors

The LM card version has two female MicroMate (also called MMCX ) antenna connectors on one end. See Figure 2-1. All antennas and cables attached to the adapter must be equipped with male MicroMate connectors.

The two antenna connectors allow a Diversity Antenna or two separate antennas to be attached to the Cisco Aironet Wireless LAN Adapter. When two antennas are connected, the adapter automatically selects antennas to provide the strongest signal for radio operations. This feature improves packet delivery and system throughput by avoiding reception and transmission instances that are hampered by RF multipath signals or blocking structures in the environment.

**Figure 2-1** LM Adapter Antenna Connections



## Attaching a Remote Antenna



**Note**

The PCM version of the adapter comes with the antenna installed. If you need to remove or change the antenna, remove the adapter from the PC card slot.

**Step 1** Line up the antenna cable leads with the connectors on the adapter.

**Step 2** Slide the cable leads into the connectors until they snap into place.



**Note**

The J1 port is the primary port. If the antenna has only 1 MMCX connector, attach it to the J1 port.

## Detaching a Remote Antenna

- 
- Step 1 Remove the adapter from the PC card slot.
  - Step 2 Grasp the end of the antenna cable lead by the connector.
  - Step 3 Gently pull the connector away from the adapter until it comes free.
- 

## Inserting the Client Adapter into a Computing Device

This section provides instructions for inserting a PC card or a PCI client adapter into a computing device.

**Caution**

---

These procedures and the physical connections they describe apply generally to conventional PC card slots and PCI expansion slots. In cases of custom or nonconventional equipment, be alert to possible differences in PC card slot and PCI expansion slot configurations.

---

## Inserting a PC Card

- 
- Step 1 Before you begin, examine the PC card. One end has a dual-row, 68-pin PC card connector. The card is keyed so that it can be inserted only one way into the PC card slot.
  - Step 2 Turn on your computer, let the operating system boot up completely, and follow the remaining steps in this section to insert the PC card.

**Caution**

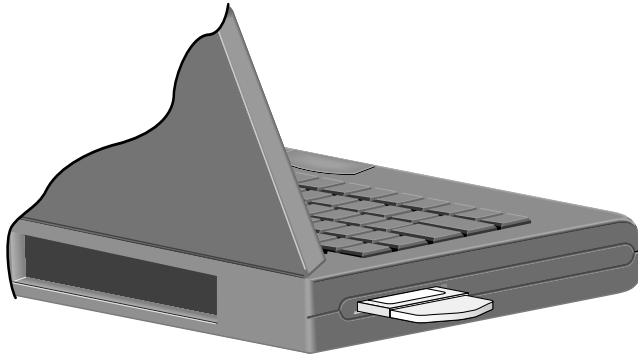
---

Do not force the PC card into your computer's PC card slot. Forcing it will damage both the card and the slot. If the PC card does not insert easily, remove the card and reinsert it.

---

- Step 3 Hold the PC card with the Cisco logo facing up and insert it into the PC card slot, applying just enough pressure to make sure it is fully seated. See Figure 2-2.
-

**Figure 2-2** Inserting a PC Card into a Computing Device



**Note**

You can remove and reinsert your PC card when necessary. See the “Removing the Client Adapter” section on page 2-7 for instructions.

## Inserting a PCI Client Adapter

- Step 1** Turn off the PC and all its components.
- Step 2** Remove the computer cover.  
On most Pentium PCs, PCI expansion slots are white. Refer to your PC documentation for slot identification.
- Step 3** Remove the screw from the top of the CPU back panel above an empty PCI expansion slot. This screw holds the metal bracket on the back panel.

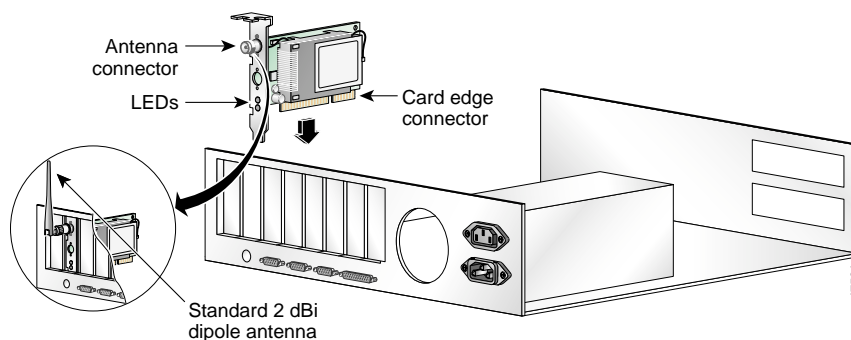


**Caution**

Static electricity can damage your client adapter. Before removing the adapter from the antistatic packaging, discharge static by touching a metal part of a grounded PC.

- Step 4** Examine the client adapter. The antenna connector and the LEDs face out of your computer and are visible when you put the cover back on. The bottom edge of the adapter is the connector that you will insert into an empty expansion slot in your computer. See Figure 2-3.

**Figure 2-3** Inserting a PCI Client Adapter into a PC



**Step 5** Tilt the adapter to allow the antenna connector and LEDs to slip through the opening in the CPU back panel.

**Step 6** Press the client adapter into the empty slot until the connector is firmly seated.



**Caution** Do not force the adapter into the expansion slot as this could damage both the adapter and the slot. If the adapter does not insert easily, remove the adapter and reinsert it.

**Step 7** Reinstall the screw on the CPU back panel, and replace the computer cover.

**Step 8** Attach the 2-dBi antenna to the adapter's antenna connector until it is finger-tight. Do *not* overtighten.

**Step 9** For optimal reception, position the antenna so that it is straight up.

**Step 10** Boot up your computer.



**Note** Because PCI adapters are installed inside desktop computers, you should have little reason to remove the adapter. However, instructions are provided in the “Removing the Client Adapter” section on page 7-7 in case you ever need to remove your PCI client adapter.

## Removing the Client Adapter

Follow the instructions in this section whenever you need to remove the client adapter from your computer.

### Removing a PC Card

To remove a PC card after it is successfully installed and configured (such as when your laptop is to be transported), pull the card directly out of the PC card slot. The client adapter is “hot swappable” and can be inserted and ejected at any time after you have installed the driver.

### Removing a PCI Client Adapter

Because a PCI adapters are installed inside desktop computers, which are not designed for portable use, you should have little reason to remove the adapter. Follow these steps in case you ever need to remove your PCI client adapter.

**Step 1** Completely shut down your computer.



**Note** When the computer is turned off by using the power switch, there still might be power supplied to the motherboard. To ensure that your computer is completely shut down, unplug the computer's power cord from its power source.

**Step 2** Disconnect the client adapter's antenna.

**Step 3** Remove the computer cover.

- Step 4** Remove the screw from the top of the CPU back panel above the PCI expansion slot that holds your client adapter.
  - Step 5** Pull up firmly on the client adapter to release it from the slot, and carefully tilt the adapter to allow it to clear the opening in the CPU back panel.
  - Step 6** Reinstall the screw on the CPU back panel, and replace the computer cover.
-



## Installing the Software

---

This chapter provides instructions on how to install the PACKET, NDIS2, NDIS3 and ODI drivers operating under MS-DOS, Windows 3.x, and Windows for Workgroups

These topics are covered in this section:

- Driver Overview, page 3-2
- Windows for Workgroups 3.11 NDIS2 Installation, page 3-3
- DOS NDIS2 Installation, page 3-3
- ODI Driver Installation, page 3-5
- Additional Requirements and Features, page 3-5
- Driver Keywords and Settings, page 3-6

# Driver Overview

This section covers the drivers. The utilities are discussed in Chapter 4, “Utilities.”

The MS-DOS and Windows for Workgroups based drivers must have a configuration file created (or edited) with an ASCII text editor.

The drivers and associated files do not ship with the adapter. You must download them from the Wireless Software Center at Cisco.com. The downloadable file, DOSDRVS.EXE, is a self-extracting executable file containing separate self-extracting executable files for each driver. After downloading and running the DOSDRVS.EXE file, you can run the driver file for your specific application. You must also run the UTIL.EXE to extract the utility programs for these drivers. The structure of the DOSDRVS.EXE file is shown in Table 3-1.

**Table 3-1** DOSDRVS.EXE File Structure

Filename	Description
DOSDRVS.EXE	A self-extracting executable file containing these self-extracting executable files: <ul style="list-style-type: none"> <li>• PKT.EXE—packet driver and files</li> <li>• ODI.EXE—ODI driver and files</li> <li>• NDIS.EXE—NDIS2 driver and files</li> <li>• UTIL.EXE—configuration and diagnostic utilities</li> <li>• DOSINST.PDF—<i>Cisco Aironet Wireless LAN Client Adapters Installation and Configuration Guide for MS-DOS</i> in portable data file format</li> </ul>
<b>PKT.EXE Files</b>	
CSCPKT.COM	Packet driver
CSCPKT.INI	Sample initialization file
READ1ST.TXT	Text file containing driver and installation notes
<b>ODI.EXE Files</b>	
CSCODI.COM	ODI driver
NET.CFG	Sample initialization file
READ1ST.TXT	Text file containing driver and installation notes
<b>NDIS.EXE Files</b>	
CSCNDIS2.DOS	NDIS driver
PROTOCOL.INI	Sample initialization file
READ1ST.TXT	Text file containing driver and installation notes
<b>UTIL.EXE Files</b>	
AWCALLID.EXE	Establishes a call id number
PCMCIA.COM	Turns the PCMCIA slot on or off to allow utilities to access the adapter
RADINFO.COM	Displays the adapter’s radio statistics
WEPDOS.EXE	Sets a WEP transmit key and key values



## Windows for Workgroups 3.11 NDIS2 Installation

- 
- Step 1 Power on your computer, and start Windows for Workgroups.
  - Step 2 Extract the NDIS.EXE files to the directory containing the network files on your computer's hard drive.
  - Step 3 Go to the Network program group, and click **Network Set-Up**.
  - Step 4 Under Network Setup, choose **Networks....**
  - Step 5 Under Networks, choose **Install Microsoft Windows Network**. Click **OK**.
  - Step 6 Under Network Setup, choose **Drivers....**
  - Step 7 Under Network Drivers, choose **Add Adapters**.
  - Step 8 If the drivers are already copied to the hard disk, they are displayed in the list.
  - Step 9 Under Add Adapter, choose the appropriate Cisco Aironet Adapter. If it is not on the menu list, choose **Unlisted or Updated Network Driver**. Choose the correct Cisco Aironet Adapter, and click **OK**.
  - Step 10 If the chosen adapter is displayed in the **Network Drivers**, click **Setup**.
  - Step 11 Select the appropriate parameters, such as Infrastructure Mode, SSID, Channel, and Bitrate.
  - Step 12 Exit Windows for Workgroups.
  - Step 13 To modify the PC Card system parameters, edit the PROTOCOL.INI file in the Windows directory.
  - Step 14 Reboot your computer.
- 

## DOS NDIS2 Installation

The Cisco Aironet Wireless LAN Adapter can be installed in a NetBIOS-compliant MS-DOS environment such as MicroSoft LAN Manager or PC LAN. The installation of this driver includes creating or editing a configuration file (PROTOCOL.INI).

This file must contain the lines shown in Table 3-2.

*Table 3-2 Minimum PROTOCOL.INI Driver Settings*

Infrastructure Mode	Ad Hoc Mode
[CSCNDIS2]	[CSCNDIS2]
DRIVERNAME = CSCNDIS2\$	DRIVERNAME = CSCNDIS2\$
INFRASTRUCTURE = YES If omitted, default is YES	INFRASTRUCTURE = NO
SSID = <your SSID>	SSID = <your SSID>
	CHANNEL = <channel>

Additional variables defined in the following section can also be used. Follow these steps to install the driver.

- 
- Step 1** Power on your computer.
  - Step 2** Extract the NDIS.EXE files to the directory containing the network files on your computer's hard drive.
  - Step 3** Copy the PROTOCOL.INI file to the network directory or merge statements from the Cisco Aironet supplied file into your existing PROTOCOL.INI file.
  - Step 4** Modify the CONFIG.SYS file. After the line containing: Device = PROTMAN.DOS, add Device = [drive:] [path] CSCNDIS2.DOS.
  - Step 5** To modify the PC Card system parameters, edit the PROTOCOL.INI file in the network directory. For a list of parameters that can be modified, see Table 3-2.
  - Step 6** Reboot your computer.
- 

## DOS Packet Driver Installation

The installation of this driver includes creating or editing a configuration file (CSCPKT.INI). This file must contain the lines shown in Table 3-3.

**Table 3-3** Minimum CSCPKT.INI Driver Settings

Infrastructure Mode	Ad Hoc Mode
[CSCPKT]	[CSCPKT]
INFRASTRUCTURE = YES If omitted, default is YES	INFRASTRUCTURE = NO
SSID = <your SSID>	SSID = <your SSID>
	CHANNEL = <channel>

Additional variables defined in the following section can also be used.

The Wireless LAN Adapter can be installed in a MS-DOS environment by using MS-DOS IP stack products such as FTP software.

Follow these steps to install the driver.

- 
- Step 1** Power on your computer.
  - Step 2** Extract the PKT.EXE files to the directory containing the network files on your computer's hard drive.
  - Step 3** Make sure that the CSCPKT.INI file is in the directory containing the Packet driver.
  - Step 4** If you would like to modify the PC Card system parameters, edit the CSCPKT.INI file. For a list of parameters that can be modified, see Table 3.3.
  - Step 5** Load the driver by typing **CSCPKT [-cinuw] <int\_number>** at the MS-DOS prompt (for example, CSCPKT 0x65) and press **Enter**.



**Note** Options -c, -i, -n, and -w are unused in this version of the driver and are provided for backward syntax compatibility.



**Note** <int\_number> is an interrupt vector location in the range 0x60 to 0x7F.



**Note** To unload the driver, enter **CSCPKT -u <int\_number>** (for example, **CSCPKT -u 0x65**). The <int\_number> value must be the same value used when you installed the driver.

**Step 6** Load the MS-DOS IP stack.

## ODI Driver Installation

The PC Card can be installed in an ODI compliant MS-DOS environment such as Novell NetWare. Follow these steps to install the driver.

- 
- Step 1** Power on your computer.
- Step 2** Extract the CSCODI.COM files to the directory containing the network files on your computer's hard drive.
- Step 3** Copy the NET.CFG file, or merge the Cisco Aironet supplied NET.CFG file into your existing NET.CFG file in the network directory.
- Step 4** Modify the adapter's system parameters by editing the NET.CFG file. The following parameters can be modified (INFRASTRUCTURE mode only):
- INFRASTRUCTURE = YES (If omitted, default is YES)
  - SSID = <your SSID>
- Step 5** Run the batch files created by the NetWare installation disks, or manually load the driver from AUTOEXEC.BAT or the command line. This can be done by running LSL, followed by CSCODI, IPXODI, and NETX or VLM.
- 

## Additional Requirements and Features

The following INI and CFG file lines might appear anywhere within a section. Only the sections containing these lines will be parsed:

- CSCPKT.INI file can have a section header of [CSCPKT].
- PROTOCOL.INI file can have any section header, but the section must contain the keyword and parameter DRIVERNAME = CSCNDIS2.
- NET.CFG file must have a section header of Link Driver CSCODI.

The following general information is pertinent:

- Multiple sections are supported.
- Blank lines are supported.
- Comments begin with semicolon and can appear anywhere on a line.
- Keywords can be uppercase or lowercase and can be surrounded by white space if desired.
- Any parameter or variable that can be set to ON or OFF can also be set to YES or NO, respectively.
- Any parameter that begins with *0x* will be assumed to be hexadecimal. Any parameter that begins with a digit (excluding the *0x* case) will be assumed to be decimal. Any parameter that begins with quotes will be assumed to be a quoted string parameter. Any other parameter will be assumed to be an unquoted string parameter.
- For string parameters, double quotes are required around the string if the string contains any special characters.



**Note**

---

The PROTOCOL.INI file does not support some of the white space characters in a quoted string. If a string begins with an alphabetic character and contains no special characters, the quotes can be omitted.

---

- For Packet string parameters, the string can be enclosed with double quotes or single quotes. If a string is quoted, any character except a “null” and the quote delimiter itself can occur between the quotes.



**Note**

---

If double quotes are used for a delimiter, a single quote can appear in the string, and vice versa. If the string begins with an alphabetic character and contains no special characters, the quotes can be omitted.

---

- For numeric parameters, the value can be hexadecimal or decimal. Hexadecimal numbers must be preceded with the characters *0x* but all characters can be uppercase or lowercase.

## Driver Keywords and Settings

The default PC Card configuration is set to:

- Constant Awake Mode.
- Infrastructure Mode—allows association with any access point matching the SSID supplied by the user.
- The factory-supplied network address.
- Receive directed packets to this address as well as multicasts and broadcasts.
- Retry data packets up to 16 times before discarding the frame.
- Retry RTS sequence up to 16 times before discarding the frame.
- RTS exchange on all frames greater than 300 bytes.
- Fragment frames longer than 700 bytes.
- Discard fragmented transmit packets if not delivered in 5 seconds.
- Discard fragmented receive frames if not complete after 10 seconds.

- Active scanning with 3-Kusec energy detect time and 20-Kusec probe response wait timeout.
- Rescan if 8 beacons are consecutively missed.
- Send an access point keep-alive message every 10 seconds.

The following tables contain keywords and parameter settings common to both the NDIS2 PROTOCOL.INI, ODI NET.CFG, and the PKT CSCPCT.INI configuration files.

## Basic System Parameters

Basic system operation can be adjusted with the following parameters.

**Table 3-4 General Network Parameters**

Parameter (Keyword)	Value	Description
INFRASTRUCTURE	ON, YES OFF, NO	(Optional)—Specifies whether system operation uses an infrastructure or peer-to-peer/ad hoc network.  Default: ON, YES
SSID	1–32 character string	Identifies the service set identifier of the specific wireless network you are connected to.  This parameter must match the system SSID.
NODENAME	1–16 character string	(Optional)—Specifies a readable name for the station.
NETADDRESS	Any IEEE MAC address except broadcast and multicast	(Optional)—Allows for locally administered MAC addresses by overriding the unique MAC ID on the adapter.
NODE ADDRESS		Same as NETADDRESS (keyword valid only in NET.CFG file).
RXMODE	NORMAL UNICAST NOMULTICAST	(Optional)—Determines what frames are delivered to the driver from the adapter. Normal means unicast, multicast, and broadcast frames are received.  Default: NORMAL
DATARATE1	0–255	(Optional)—Specifies the rate at which the adapter communicates with the access point to which it associates.  Default: 1–11  This setting must match the access point's setting.
DATARATE2	0–255	

## Network Performance Variables

Network performance can be optimized with the following variables.

**Table 3-5** *Advanced Network Variables*

Variable	Value	Description
LONGRETRYLIMIT	0–255	(Optional)—Specifies the number of times an unfragmented packet is retried before it is dropped and a transmit error is reported to the driver.  Default: 16
SHORTRETRYLIMIT	0–255	(Optional)—Specifies the number of times a fragmented packet is retried to gain access before it is dropped and a transmit error is reported to the driver.  Default: 16
RTSTHRESHOLD	0–2312	(Optional)—specifies the minimum frame size in bytes for which RTS/CTS delivery are used. Packets longer than the specified value are delivered by using RTS/CTS handshaking.  Default: 300
TXMSDULIFETIME	0–0xFFFF	(Optional)—Specifies the maximum time to attempt packet delivery.  Default: 5000 kus (5 seconds)
RXMSDULIFETIME	0–0xFFFF	(Optional)—Specifies the maximum time for receiving a fragmented packet.  Default: 10000 kus (10 seconds)
TXPOWERLEVEL	0–100	(Optional)—Selects the programmed transmit power level in mW, which can vary per country.
DIVERSITY	DEFAULT ON RIGHT LEFT	(Optional)—Specifies the transmit or receive diversity method used by the adapter.  Default = Diversity is turned on On = Adapter uses both antennas Right = Adapter uses the antenna attached to jack 1 Left = Adapter uses the antenna attached to jack 2  Default: ON
LEAP	ON (YES) OFF (NO)	(Optional)—turns LEAP (Cisco's version of Extensible Authentication Protocol) on or off.  Default: OFF

**Table 3-5** *Advanced Network Variables (continued)*

Variable	Value	Description
WORLDMODE	ON (YES) OFF (NO)	(Optional)—Allows the adapter to automatically inherit channel configuration and output power properties from the access point to which it associates. Default: OFF (NO) Enable World mode when the adapter needs to automatically match the country configuration of the access point to which it associates.
SHORTPREAMBLE	0, 1, 2	(Optional)—Establishes the length of the packet's synchronization bit. Default: 0 0 = Automatic 1 = Long preamble 2 = Short preamble

## Fragmentation Variables

Additional system performance adjustments can be made with the following group of variables.

**Table 3-6** *Fragmentation Variables*

Variable	Value	Description
FRAGTHRESHOLD	256–312 (must be an even value)	(Optional)—Specifies the fragmentation size in bytes. Frames longer than the specified value are transmitted using multiple packets. Default: 700

## Power Management Variables

The Wireless LAN Adapter power management can be adjusted with the following group of variables.

**Table 3-7 Power Management Variables**

Variable	Value	Description
POWERSAVEMODE	CAM PSP FASTPSP	<p>(Optional)—Establishes the operating method the device uses to conserve electrical power.</p> <p>CAM = Constant Awake Mode PSP = Power Save Mode FASTPSP = Fast Power Save Mode</p> <p>Default: CAM</p> <p>In ad hoc mode, if the POWERSAVEMODE is PSP or FASPSP, the ATIMDURATION variable must be a non-zero value.</p> <p>CAM keeps the client adapter powered up continuously so there is little lag in message response time. This mode consumes the most power but offers the highest throughput.</p> <p>PSP powers the adapter on and off based on a time algorithm. When retrieving packets, the adapter remains in PSP mode and manages only the amount of traffic within the time period when it is scheduled on. When the time expires, the adapter turns off for the required time and then turns back on again to retrieve more data.</p> <p>FASTPSP switches between a PSP mode and CAM, depending on network traffic. This mode switches to CAM when retrieving a large number of packets and switches back to PSP after the packets have been retrieved.</p>
MAXPOWERSAVE	ON (YES) OFF (NO)	<p>(Optional)—Turns Maximum Power Save mode on or off.</p> <p>Default: OFF</p> <p>MAXPOWERSAVE causes the access point to buffer incoming messages for the client adapter, which wakes up periodically and polls the access point to see if any buffered messages are waiting for it. The adapter can request each message and then go back to sleep.</p> <p>MAXPOWERSAVE conserves the most power but offers the lowest throughput. Is recommended for devices for which power consumption is the ultimate concern (such as small battery-powered devices).</p>



Table 3-7 Power Management Variables (continued)

Variable	Value	Description
ATIMDURATION	Between 0 and less than the beacon interval	(Optional)—Specifies the length of time for ATIMs following a beacon. Default: 5 Kusec Constant Awake Mode is 0. In ad hoc mode, this value must be non-zero if POWERSAVEMODE is PSP or FASTPSP. This value is used only when starting a new network. When joining a network, the value currently in use is adopted.
SLEEPFORDTIM	ON (YES) OFF (NO)	(Optional)—Allows the node to sleep through DTIMs for extra power saving. Broadcast and multicast traffic might be missed. Default: OFF Used only in INFRASTRUCTURE mode when POWERSAVE mode is PSP or FASTPSP.
LISTENTIME	0–0xFFFF	(Optional)—Determines how often to awaken for beacons. Default: 200 Kusec (200 ms) Used only in INFRASTRUCTURE mode when POWERSAVE mode is PSP or FASTPSP. The PC card always awakens to receive DTIMs when in PSP Mode, unless sleep for DTIMs is set.
FASTLISTENTIME	0–0xFFFF	(Optional)—Determines how often to awaken for beacons. default: 100 Kusec (100 ms) Used only in INFRASTRUCTURE mode when POWERSAVE mode is PSP or FASTPSP. The PC Card always awakens to receive DTIMs when in FASTPSP Mode.

Table 3-7 Power Management Variables (continued)

Variable	Value	Description
LISTENDECAY	0–0xFFFF	(Optional)—Specifies the rate at which the listen interval grows.  Default: 2  Used only in INFRASTRUCTURE mode when POWERSAVE mode is PSP or FASTPSP.  Listen interval begins at FASTLISTENTIME and eventually decays to LISTENTIME.
FASTLISTENDELAY	0–0xFFFF	(Optional)—Specifies the time to delay immediately after a transmission before beginning at FASTLISTENTIME.  Default: 200 Kusec (200ms)  Used only in INFRASTRUCTURE mode when POWERSAVE mode is PSP or FASTPSP.

## Scanning Variables

Additional system performance adjustments can be made with the following group of variables.

Table 3-8 Scanning Variables

Variable	Value	Description
SCANMODE	ACTIVE, PASSIVE, ADVANCED	(Optional)—Determines the current scanning mode used by the adapter.  Default: ACTIVE
BEACONLISTENTO	0–0xFFFF	(Optional)—Determines the amount of time to listen for a beacon on each channel.  Default: 40 Kusec  Used only if SCANMODE = PASSIVE
PROBEENERGYTO	0–0xFFFF	(Optional)—Determines the amount of time to listen for RF energy following a probe.  Default: 3 Kusec  Used only if SCANMODE = ACTIVE
PROBERESPONSETO	0–0xFFFF	(Optional)—Determines the amount of time to wait for a probe response after energy is detected on a channel.  Default: 20 Kusec  Used only if SCANMODE = ACTIVE

**Table 3-8 Scanning Variables (continued)**

Variable	Value	Description
STATIONARY	ON, OFF, YES, NO	(Optional)—indicates whether or not the station is mobile. Default: OFF
PROBEDELAY	0–0xFFFF	(Optional)—Indicates how long to wait on a frequency before sending a probe request. Default: 3 Kusec
OFFSCANINTERVAL	0–0xFFFF	(Optional)—Determines how often to attempt to use the off-line scanning method to search for new access points. Default: 0 (which disables off-line scanning)
OFFSCANDURATION	0–0xFFFF	(Optional)—Determines how long to use the off-line scanning method during each attempt. Default: 0 (disables off-line scanning)

## Infrastructure Parameters

Additional system performance adjustments can be made with the following parameters.

**Table 3-9 Infrastructure Parameters**

Parameter	Value	Description
SSID	1 to 32 character string	Establishes the adapter's service set identifier. This parameter must match the SSID of the system for proper infrastructure operation. Default: tsunami
BEACONLOSTTIME	0–0xFFFF	(Optional)—Determines the interval of consecutively missed beacons which will cause a rescan. Default: 500 Kusec
REFRESHINTERVAL	0–0xFFFF	(Optional)—Determines the amount of time in seconds between refresh packets to the access point. Use 0xFFFF to disable Default: 10,000 Kusec (10 sec)
SPECIFIEDAP	Any IEEE MAC address except broadcast and multicast	(Optional)—Forces association to the specified access point.
SPECIFIEDAP2	Any IEEE MAC address except broadcast and multicast	(Optional)—Forces association to one of the specified access points.

Table 3-9 Infrastructure Parameters (continued)

Parameter	Value	Description
SPECIFIEDAP3	Any IEEE MAC address except broadcast and multicast	(Optional)—Forces association to one of the specified access points.
SPECIFIEDAP4	Any IEEE MAC address except broadcast and multicast	(Optional)—Forces association to one of the specified access points.
SPECIFIEDAPTO	0–0xFFFF	(Optional)—Establishes the time to attempt to associate to a specified access point before searching for any available access points (with matching SSID). Default: 10,000 Kusec (10 sec)
AUTHTIMEOUT	0–0xFFFF	(Optional)—Establishes the time to attempt to authenticate to an access point. Default: 2,000 Kusec (2 sec)

Table 3-9 Infrastructure Parameters (continued)

Parameter	Value	Description
AUTHTYPE	OPEN, WEPOPEN WEP SHARED MIXED OPEN MIXED SHARED	<p>(Optional)—Determines the wireless network's level of security.</p> <p>OPEN = Allows client, regardless of its WEP settings, to authenticate and attempt to communicate with an access point.</p> <p>WEPOPEN = Client uses full encryption. Access point Encryption by Station parameter must be set to full encryption and Accept Authentication Type parameter set to Open.</p> <p>WEP SHARED = Client uses full encryption. Access point Encryption by Station parameter must be set to Full Encryption and Accept Authentication Type parameter set to Open.</p> <p>MIXED OPEN = Client can operate in a cell with other clients regardless of encryption used. Access point Encryption by Station parameter must be set to open, Authentication Accept Type parameter set to Open.</p> <p>MIXED SHARED = Client can operate over a range of cells with other clients regardless of encryption used. Access Point Encryption by Station parameter must be set to optional, and Accept Authentication Type parameter must be set to shared.</p> <p>Default: OPEN</p> <p>This parameter is not available in ad hoc mode.</p>
ASSOCIATIONTO	0–0xFFFF	<p>(Optional)—Shows the maximum amount of time that the client waits for a response to an association request from the access point.</p> <p>Default: 2,000 Kusec (2 sec)</p>

## Ad Hoc Variables

Ad hoc system operation is accomplished with this group of variables.

*Table 3-10 Ad Hoc Variables*

Variable	Value	Description
JOINNETTO	0–0xFFFF	(Optional)—Determines the amount of time that an ad hoc station scans before starting its own network.  Default: 10,000 Kusec (10 sec)
BEACONPERIOD	0–0xFFFF	(Optional)—Specifies the beaconing interval.  Default: 100 Kusec
DSCHANNEL	0–14	(Optional)—This variable is valid only for a node that starts a network. This is the channel identifier specifying the frequency to communicate on. For all other nodes, the radio will scan for the proper frequency.  Default: 0 (which will cause the radio to pick a default channel appropriate for its programmed carrier set)  Any other value (1 to 14) is validated against the programmed carrier set and rejected if invalid.
ATIMDURATION	Between 0 and less than the beacon interval	(Optional)—Specifies the length of time for ATIMs following a beacon.  Default: 5 Kusec  Constant Awake Mode is 0.  In ad hoc mode, this value must be non-zero if POWERSAVEMODE is PSP or FASTPSP.  This value is only used when starting a new network. When joining a network, the value currently in use is adopted.

## Adapter Keywords

The following is a list of keywords that control the host system hardware resources the Cisco Aironet Wireless LAN Adapter requires.



### Note

At a minimum, the adapter requires 64 consecutive 16-bit I/O ports, one nonsharable Interrupt and one PC Card type II slot.

If you are using card services, these resources are assigned for you. However, you can override the card services resource assignments by including the PortBase or INT/IRQ keywords in the appropriate configuration file.

If you are not using card services, your host system must have an Intel 82365 or compatible PC Card controller chip. The driver then configures the PC Card controller chip directly, and each of the following parameters should be specified in your configuration file.

**Table 3-11 Adapter Keywords**

Keyword	Value	Description
PORTBASE	0–0xFFFF	(Optional)—Specifies the starting address for a block of 32 consecutive 16-bit I/O ports. Make sure the block of I/O addresses does not overlap the address of another device in the machine. This can be used to override a card service assignment.  Default: 0x140 (if card services are not used)  The starting PORTBASE address must be on an even 0x40 byte boundary.
PORT	0–0xFFFF	Only valid in NET.CFG file (same as PORTBASE).
INT	2–15	(Optional)— Specifies the hardware interrupt the PC Card uses. The Interrupt must be unique (not used by another device in the machine). Use this keyword to override a card service assignment.  Default: 11 (if card services are not used)
IRQ	2–15	Same as INT.
SOCKET	0–7	(Optional)— Ignored if card services are used. If card services are not used, this is the PC Card socket the PC Card is inserted in.  Default: 0
MEMORY	0xC000–0xDF00	(Optional)—Ignored if If card services are used. If card services are not used, this is a block of memory the driver uses to view the PC Card CIS.  Default: 0xD000  In the NET.CFG file, the parameter is D0000, not 0xD000.
MEM	0xC00–0xDF00	Same as MEMORY.







## Utilities

---

This section describes procedures for using utilities and updating firmware depending on the operating system used.

These topics are covered in this section:

- Site Survey and Link Test, page 4-2
- Loading New Firmware Versions, page 4-3
- DOS Utilities, page 4-3

## Site Survey and Link Test

To perform a meaningful site survey, you need to conduct a test that accurately models the intended use of the system. It is important to perform a site survey using equipment that is similar to that implemented. Survey these items:

- Transmit power
- Antennas and types
- Antennas and locations
- Packet (fragment) size
- Interference

Conduct the site survey with all variables set to the operational values. You should also perform it during the time the RF link is generally functioning with all other systems and noise sources operational. For efficiency, execute the site survey application entirely from the mobile station.

The link test tool helps determine the RF network coverage. The results of the link test help eliminate low RF signal level areas that can result in loss of connection between the PC Card and the access point.

It is important to remember that the information being displayed is from the access point viewpoint. Therefore, packets sent are from the access point to the PC Card client. Packets received are from the PC Card to the access point. Signal quality is an estimate of the signal strength recorded at the time of packet reception by the radio.

## Using Windows 3.11 or DOS to Perform a Link Test Using Telnet



### Note

---

For additional information about performing link tests, refer to the documentation for the access point your system is using.

---

Link test through a Telnet session/connection is a useful tool for determining:

- Coverage range of an access point
- Communication range of stations/mobile stations

Follow these steps to perform the link test using a Telnet session.

- 
- Step 1** Install the drivers.
  - Step 2** Configure the drivers for network operation.
  - Step 3** Ensure that mobile or portable PC Card devices and the access point have unique IP assignments.
  - Step 4** Set up an access point for the intended operation (set fragmentation thresholds, RTS thresholds, and so on.)
  - Step 5** Start the operating system on the mobile station.
  - Step 6** Configure the adapter.
  - Step 7** Make sure the mobile station is associated to the access point.
  - Step 8** Start a Telnet session on the mobile station to the access point. Depending on the system in use, the Telnet application might have logging and note taking capability. If so, enable these modes.

- Step 9** Navigate through the access point menu to the link test option. See the appropriate access point technical reference manual for more information.
- Step 10** Set up the test options to accurately model the system.
- Step 11** Set the test for continuous operation with a 1-second delay.
- Step 12** Begin traversing the area around the access point to determine its coverage. If logging and notes are not possible with the Telnet application, maintain a manual log.

---

The Telnet session packets are interspersed with test packets that might increase the round trip time for some frames. The link test will show progress changes as the test is being conducted.

The first-time delivery success rate for the packet cannot be important for transaction based systems and can result in a slightly larger range. Using longer packets can provide some degree of safety margin in the range estimate.

**Note**

---

Roundtrip time is affected by the Telnet session maintenance.

---

## Loading New Firmware Versions

We recommend that you use the Cisco Windows-based Aironet Client Utility (ACU) for your firmware updates. After updating the firmware by this method, you can reinstall the adapter in its MS-DOS computing device.

## DOS Utilities

This section describes the MS-DOS utility programs used to perform configuration and diagnostics of the Cisco Aironet wireless LAN client adapters. The programs work on the PCM34x, LMC34x, PCM35x, and LMC35x. The programs cannot work on older cards, depending on the hardware features and firmware levels of those cards.

## Configuration Utilities

The configuration programs update the firmware of the card. First unload any protocol driver. These configuration utilities are shipped with the drivers:

- WEPDOS.EXE—sets a WEP transmit key and key values
- AWCALLID.EXE—establishes a call ID number

The following utility does not ship with the drivers. To obtain it, contact your local Cisco System Engineer.

- AWCLEAP.EXE—sets and clears LEAP username and passwords

## Diagnostic Utilities

The following diagnostic utility ships with the drivers:

- PCMCIA.COM—turns the PCMCIA slot on so that the other utilities can access the adapter. The utility also turns the slot off.
- RADINFO.EXE—displays the adapter's radio statistics

## DOS Utilities Running Environment

The DOS utilities run well under MS-DOS 6.22.

For the PCM350 and LM350 PCMCIA cards, the DOS utilities do not use card and socket services for configuring the cards; they program the PCMCIA socket directly. Therefore, an 82365-compatible socket controller is required for proper operation. Many, but not all, socket controllers have this capability.



**Note**

If a utility program does not run, use the PCMCIA.COM utility to turn the adapter's slot on. After you are finished running the utility programs, use PCMCIA.COM to turn the adapter's slot off.

## Layout and Format

Information on each utility in this section is presented in the following format:

<b>Description</b>	This section contains a general description of the utility and how it is used.
<b>Syntax</b>	The correct syntax is shown in this section in the following format:  COMMAND [-option] [-option]
<b>Options</b>	Available options are listed here with a brief description of their purpose.
<b>Standard Options (Default settings in brackets)</b>	The following options are considered standard options because they are common to the utilities that require their use: <p>-p[IO base]            IO base address (hex) [380]          -io# -misa# -isa#    IO type, #={8 16}          -b [membase]        Memory base address (hex) [D000:0]          -I [irq]             Interrupt request (decimal) [5]          -s [slot]            Slot number (decimal) [0]          -365                 82365 card startup          -pci                 PCI card startup;          -nocheck            I/O access not tested on startup</p> <p>Standard options are available when they are displayed as part of the command or when using the help (-?) option.</p>
<b>Remarks</b>	This section contains information about the utility that can help the user.

## General Usage Notes

### Syntax

The utility does not run unless its command syntax is correct. In most cases, an error message appears, informing you that the command or option was invalid.

The `-pci` switch activates the utility's PCI card startup feature. Use this switch when you have a PC card client or an LM client running in a PCI carrier card.

## Running the Utilities

The utilities are started by entering the appropriate command and options at the command prompt and pressing **Enter**. The following general guidelines might be helpful.

When a utility has standard options:

- Enter the card startup switch (`-365`) as the first option. This option informs the utility to start the adapter.
- The default IO base address (`0x380`) works in most cases, depending on the platform on which you are running the utilities. If the utility reports problems accessing the card's registers, you might need to move this window. The card requires a contiguous 64-byte I/O window to work properly.
- The default base address (`D000:0000`) is used to access the card's PCMCIA configuration registers and enable the card interface. A 2-Kb window is required.
- The default IRQ (`5`) also works in most cases, depending on the platform on which you are running the utilities. Most of the utilities do not actually require the use of an interrupt.

## Getting Help

Use the `-?` option to display a brief explanation of the utility and its command syntax.

## Configuration Utilities

### AWCLEAP.EXE

<b>Description</b>	Sets the LEAP username and password																
<b>Syntax</b>	AWCLEAP [username noname] password [-clear] [-d]																
<b>Options</b>	<table> <tr> <td>username</td> <td>Sets a username</td> </tr> <tr> <td>-noname</td> <td>Disables the username feature</td> </tr> <tr> <td>password</td> <td>Sets a LEAP password</td> </tr> <tr> <td>-clear</td> <td>Clears current username and password</td> </tr> <tr> <td>-d</td> <td>Displays current settings</td> </tr> </table>	username	Sets a username	-noname	Disables the username feature	password	Sets a LEAP password	-clear	Clears current username and password	-d	Displays current settings						
username	Sets a username																
-noname	Disables the username feature																
password	Sets a LEAP password																
-clear	Clears current username and password																
-d	Displays current settings																
<b>Standard Options (Default settings in brackets)</b>	<table> <tr> <td>-p[IO base]</td> <td>IO base address (hex) [380]</td> </tr> <tr> <td>-io# -misa# -isa#</td> <td>IO type, #={8 16}</td> </tr> <tr> <td>-b [membase]</td> <td>Memory base address (hex) [D000:0]</td> </tr> <tr> <td>-I [irq]</td> <td>Interrupt request (decimal) [5]</td> </tr> <tr> <td>-s [slot]</td> <td>Slot number (decimal) [0]</td> </tr> <tr> <td>-365</td> <td>82365 card startup</td> </tr> <tr> <td>-pci</td> <td>PCI card startup</td> </tr> <tr> <td>-nocheck</td> <td>I/O access not tested on startup</td> </tr> </table>	-p[IO base]	IO base address (hex) [380]	-io# -misa# -isa#	IO type, #={8 16}	-b [membase]	Memory base address (hex) [D000:0]	-I [irq]	Interrupt request (decimal) [5]	-s [slot]	Slot number (decimal) [0]	-365	82365 card startup	-pci	PCI card startup	-nocheck	I/O access not tested on startup
-p[IO base]	IO base address (hex) [380]																
-io# -misa# -isa#	IO type, #={8 16}																
-b [membase]	Memory base address (hex) [D000:0]																
-I [irq]	Interrupt request (decimal) [5]																
-s [slot]	Slot number (decimal) [0]																
-365	82365 card startup																
-pci	PCI card startup																
-nocheck	I/O access not tested on startup																
<b>Remarks</b>	<p>The card startup option (-365) is required to run this utility.</p> <p>This utility is not shipped with the drivers. To obtain it, contact your local Cisco System Engineer.</p>																

## AWCALLID.EXE

<b>Description</b>	Programs and displays the adapter's call ID assignment.
<b>Syntax</b>	AWCALLID [callid] [-clear] [-d]
<b>Options</b>	<p>callid                    A 12-digit decimal number assigned by the MKK.</p> <p>-clear                    Clears the current callid</p> <p>-d                         Displays the current callid</p>
<b>Standard Options (Default settings in brackets)</b>	<p>-p[IO base]                IO base address (hex) [380]</p> <p>-io# -misa# -isa#        IO type, #={8 16}</p> <p>-b [membase]              Memory base address (hex) [D000:0]</p> <p>-I [irq]                    Interrupt request (decimal) [5]</p> <p>-s [slot]                  Slot number (decimal) [0]</p> <p>-365                        82365-card startup</p> <p>-pci                        PCI-card startup</p> <p>-nocheck                  I/O access not tested on startup</p>
<b>Remarks</b>	<p>The card startup option (-365) is required to run this utility.</p> <p>If no call id is entered, or the call id is invalid, the following error message appears:</p> <pre>ERROR: Invalid Callid or problem accessing LM350</pre> <p>A valid call ID produces this message:</p> <pre>Callid:&lt;callid string&gt;</pre> <p><b>Note</b> This program is only required in Japan and only when the adapter is used in a legacy network.</p>

## AWCALLID.EXE

<b>Description</b>	Programs and displays the adapter's call ID assignment.
<b>Syntax</b>	AWCALLID [callid] [-clear] [-d]
<b>Options</b>	<p>callid                    A 12-digit decimal number assigned by the MKK.</p> <p>-clear                    Clears the current callid</p> <p>-d                         Displays the current callid</p>
<b>Standard Options (Default settings in brackets)</b>	<p>-p[IO base]                IO base address (hex) [380]</p> <p>-io# -misa# -isa#        IO type, #={8 16}</p> <p>-b [membase]              Memory base address (hex) [D000:0]</p> <p>-I [irq]                    Interrupt request (decimal) [5]</p> <p>-s [slot]                   Slot number (decimal) [0]</p> <p>-365                        82365-card startup</p> <p>-pci                        PCI-card startup</p> <p>-nocheck                  I/O access not tested on startup</p>
<b>Remarks</b>	<p>The card startup option (-365) is required to run this utility.</p> <p>If no call id is entered, or the call id is invalid, the following error message appears:</p> <pre>ERROR: Invalid Callid or problem accessing LM350</pre> <p>A valid call ID produces this message:</p> <pre>Callid:&lt;callid string&gt;</pre> <p><b>Note</b> This program is only required in Japan and only when the adapter is used in a legacy network.</p>



## WEPDOS.EXE

<b>Description</b>	Selects a transmit key index
<b>Syntax</b>	WEPDOS [-tx#] [ascii] [hex] [-key#] [home] [-d]
<b>Options</b>	<p>-tx#                   Selects the transmit key index (1,2,3,or 4) for enterprise networking</p> <p>ascii                   A 5-character ASCII string</p> <p>hex                     A 10-character hex digit string</p> <p>-key#                  Default key index: 1, 2, 3, or 4</p> <p>home                    Selects the key for use with home access points</p> <p>-d                      Displays current settings</p>
<b>Standard Options (Default settings in brackets)</b>	<p>-p[IO base]            IO base address (hex) [380]</p> <p>-io# -misa# -isa#     IO type, #={8 16}</p> <p>-b [membase]          Memory base address (hex) [D000:0]</p> <p>-I [irq]                Interrupt request (decimal) [5]</p> <p>-s [slot]              Slot number (decimal) [0]</p> <p>-365                    82365-card startup</p> <p>-pci                    PCI-card startup</p> <p>-nocheck              I/O access not tested on startup</p>
<b>Remarks</b>	<p>The card startup option (-365) is required to run this utility.</p> <p>This example shows the display after setting the transmit key index to #1 and then using the display (-d) option:</p> <pre>C:&gt;WEPDOS -365 -p180 -tx1 Setting transmit key index to 1 C:&gt;WEPDOS -365 -p180 -d WEP128 encryption is enabled. Enterprise and home networking is supported. Firmware supports four keys. C:\&gt;</pre>

## Diagnostic Utilities

### PCMCIA.COM

<b>Description</b>	Turns the PCMCIA slot on or off so that the utility programs can access and communicate with the card.	
<b>Syntax</b>	PCMCIA [ON   OFF] [-SLOT0  -SLOT1] [-TITAN] [-BASE <addr>] [-LOAD] [-BOOT]	
<b>Options</b>	ON  OFF	Enables or disables the specified PCMCIA slot.
	-SLOTn	Identifies the slot to turn on or off.
	-TITAN	Not used with 340 or 350 series adapters.
	-BASE <addr>	Base address for the memory window used to access the PCMCIA configuration space. This must point to an unused 2-Kb block in the host system memory space.
	-LOAD	Used to load new firmware.
	-BOOT	Turns on the PCMCIA slot so the other utility programs can access the adapter.
<b>Standard Options (Default settings in brackets)</b>	-p[IO base]	IO base address (hex) [380]
	-io# -misa# -isa#	IO type, #={8 16}
	-b [membase]	Memory base address (hex) [D000:0]
	-I [irq]	Interrupt request (decimal) [5]
	-s [slot]	Slot number (decimal) [0]
	-365	82365-card startup
	-pci	PCI-card startup
	-nocheck	I/O access not tested on startup
	Standard options are available when they are displayed as part of the command or when using the help (-?) option.	
<b>Remarks</b>	Use this utility to activate the adapter's slot when the other utility programs do not work and to turn it off when finished running the utility programs. The following example shows the proper command syntax to turn the slot on, run a utility program, and turn the card off:	
	<pre>PCMCIA ON -BOOT RADINFO PCMCIA OFF</pre>	

## RADINFO.EXE

<b>Description</b>	Displays the card's radio configuration.						
<b>Syntax</b>	RADINFO [-pci] [SLOT0 SLOT1] [-BASE <addr>]						
<b>Options</b>	<table> <tr> <td>-pci</td> <td>PCI card startup</td> </tr> <tr> <td>SLOTn</td> <td>Identifies the slot in which the card resides.</td> </tr> <tr> <td>BASE &lt;addr&gt;</td> <td>Base address for the memory window used to access the PCMCIA configuration space. This must point to an unused 2-Kb block in the host system-memory space.</td> </tr> </table>	-pci	PCI card startup	SLOTn	Identifies the slot in which the card resides.	BASE <addr>	Base address for the memory window used to access the PCMCIA configuration space. This must point to an unused 2-Kb block in the host system-memory space.
-pci	PCI card startup						
SLOTn	Identifies the slot in which the card resides.						
BASE <addr>	Base address for the memory window used to access the PCMCIA configuration space. This must point to an unused 2-Kb block in the host system-memory space.						
<b>Standard Options (Default settings in brackets)</b>	None						
<b>Remarks</b>	<p>This is a typical RADINFO information display:</p> <pre>C:&gt;RADINFO RADINFO Radio Information - Rev 1.47 I/O Base Address: 0x180 Product Code: Mercury Hardware Version: Rev. B1 Processor Version: A503 Bootblock Revision: Rev. 1.50 Firmware Revision: Rev. 4.23 MAC Address: 04 40 96 47 93 E5 C:\&gt;</pre>						





## Error Messages and Trouble Shooting

---

The wireless LAN client adapter provides LED messages and error codes. This section provides the general procedures for correcting common problems encountered when installing the PC Card system.

These topics are covered in this section:

- [Accessing the Latest Troubleshooting Information, page 5-2](#)
- [Interpreting the Indicator LEDs, page 5-2](#)
- [If Your Radio Fails to Establish Contact, page 5-3](#)

## Accessing the Latest Troubleshooting Information

This chapter provides basic troubleshooting tips for your client adapter. For more up-to-date and complex troubleshooting information, refer to the TAC web site at <http://www.cisco.com/tac>. Select **Wireless Technologies** under Top Issues.

## Interpreting the Indicator LEDs

The client adapter shows messages and error conditions through its two LEDs:

- Link Integrity/Power LED (green)— This LED is on when the client adapter is receiving power and blinks slowly when the adapter is linked with the network.
- Link Activity LED (amber)—This LED blinks quickly when the client adapter is receiving or transmitting data and blinks in a repeating pattern to show an error condition.

Table 5-1 interprets the LED operating messages.

**Table 5-1 LED Operating Messages**

	Green LED	Amber LED	Condition
<b>Normal Operation</b>	Blinking quickly	Blinking quickly	Power is on, self-test is OK, and client adapter is scanning for a network.
	Blinking slowly	Blinking quickly	Client adapter is associated to an access point.
	Continuously on or blinking slowly	Blinking	Client adapter is transmitting or receiving data while associated to an access point.
	Off	Blinking quickly	Client adapter is in power save mode.
	On continuously	Blinking quickly	Client adapter is in ad hoc mode.
<b>Error Conditions</b>	Off	Off	Client adapter is not receiving power, or an error has occurred.
	Off	1 blink at 2-second rate	RAM failure. Refer to the “Obtaining Technical Assistance” section in the Preface for technical support information.
	Off	2 fast blinks, 2-second pause	Flash boot block checksum failure. Refer to the “Obtaining Technical Assistance” section in the Preface for technical support information.
	Off	3 fast blinks, 2-second pause	Firmware checksum failure. Reload the firmware.
	Off	4 fast blinks, 2-second pause	MAC address error (error reading MAC chip). Reload the firmware.
	Off	5 fast blinks, 2-second pause	PHY access error. Refer to the “Obtaining Technical Assistance” section in the Preface for technical support information.
	Off	6 fast blinks, 2-second pause	Incompatible firmware. Load the correct firmware version.

## If Your Radio Fails to Establish Contact

- Change your location or the location of the antenna by a few feet and try again.
- Make sure the antenna is securely attached.
- Make sure the adapter is properly installed.
- Make sure the receiving equipment is turned on and operating.
- Make sure the receiving equipment is properly connected to the host computer.
- Check that all parameters are set properly for both the adapter and the access point.

If the radio still fails to establish contact, see the “Accessing the Latest Troubleshooting Information” section on page 5-2.







## Technical Specifications

---

This appendix provides technical specifications for the Cisco Aironet Wireless LAN Client Adapters.

These topics are covered in this section:

- Physical Specifications, page A-2
- Radio Specifications, page A-2
- Antenna Specifications, page A-4
- Power Specifications, page A-4
- Safety and Regulatory Compliance, page A-5

# Technical Specifications

Table A-1 lists the technical specifications for the Cisco Aironet Wireless LAN Client Adapters.

If a distinction is not made between series or client adapter type, the specification applies to all Cisco Aironet Wireless LAN Client Adapters in the 340 and 350 series

**Table A-1** *Technical Specifications for the Cisco Aironet Wireless LAN Client Adapters*

## Physical Specifications

Physical Dimensions (H x W x D)	
PC card	0.2 x 2.1 x 4.5 in. (0.5 x 5.4 x 11.3 cm)
LM card	0.2 x 2.1 x 3.4 in. (0.5 cm 5.4 cm 8.6 cm)
PCI client adapter	0.5 x 3.2 x 5.8 in. (1.3 x 8.1 x 14.7 cm)
Weight	
PC card and LM card	1.3 oz (0.037 kg)
PCI client adapter	4.6 oz (0.13 kg)
Enclosure	
PC card	Extended Type II PC card
LM card	Standard Type II PC card with RF connectors
Connector	
PC card and LM card	68-pin PCMCIA
PCI client adapter	PCI card edge
Status indicators	Green and amber LEDs; see Chapter 4
Operating temperature	
340 series adapters	32 to 158°F (0 to 70°C)
350 series adapters	-22 to 158°F (-30 to 70°C)
Storage temperature	-40 to 185°F (-40 to 85°C)
Humidity (nonoperational)	95% relative humidity
Altitude	<b>Operational</b> 9,843 ft (3000 m.) at room temperature for 2 hours <b>Non-operational</b> 5,000 ft (1524 m.) at room temperature for 20 hours
ESD	15 kV (human body model)
Radio Specifications	
Type	Direct Sequence Spread Spectrum IEEE 802.11b compliant

**Table A-1 Technical Specifications for the Cisco Aironet Wireless LAN Client Adapters (continued)**

Power output	
340 PC card	30 mW (15 dBm) 1 mW (0 dBm)
340 LM card	30 mW (15 dBm) (0.5 mW/MHz) 5 mW (7 dBm) (0.5 mW/MHz)
340 PCI client adapter	30 mW (15 dBm) 15 mW (11 dBm) 5 mW (7 dBm) 1 mW (0 dBm)  <b>Note</b> 30 mW is the maximum power level supported by 340 series adapters.  <b>Note</b> See page B-3 for limitations on radiated power (EIRP) levels in the European community and other countries.
350 PC and LM card	100 mW (20 dBm) 50 mW (17 dBm) 30 mW (15 dBm) 20 mW (13 dBm) 5 mW (7 dBm) 1 mW (0 dBm)
350 PCI client adapter	100 mW (20 dBm) 50 mW (17 dBm) 30 mW (15 dBm) 20 mW (13 dBm) 1 mW (0 dBm)
Operating frequency	2.4 to 2.497 GHz (depending on the regulatory domain in which the client adapter is used)
Usable channels	2412 to 2484 MHz in 5-MHz increments
Interference rejection	-35 dBc adjacent channel rejection
Data rates	1, 2, 5.5, and 11 Mbps
Modulation	Binary Phase Shift Keying (BPSK)-1 Mbps Quaternary Phase Shift Keying (QPSK)-2 Mbps Complementary Code Keying (CCK)-5.5 and 11 Mbps
Receiver sensitivity	
340 series adapters	-90 dBm at 1 Mbps -88 dBm at 2 Mbps -87 dBm at 5.5 Mbps -83 dBm at 11 Mbps
Receiver sensitivity	
350 series adapters	-94 dBm at 1 Mbps -91 dBm at 2 Mbps -89 dBm at 5.5 Mbps -85 dBm at 11 Mbps

**Table A-1** Technical Specifications for the Cisco Aironet Wireless LAN Client Adapters (continued)

Receiver delay spread (multipath)	500 ns at 1 Mbps 400 ns at 2 Mbps 300 ns at 5.5 Mbps 140 ns at 11 Mbps (350 series adapters) 70 ns at 11 Mbps (340 series adapters)
<b>Range</b>	
340 series adapters	<p><b>Outdoor</b> 1,500 ft (457.2 m) at 1 Mbps 1,200 ft (365.8 m) at 2 Mbps 800 ft (243.8 m) at 5.5 Mbps 400 ft (121.9 m) at 11 Mbps</p> <p><b>Indoor</b> 300 ft (91.4 m) at 1 Mbps 225 ft (68.6 m) at 2 Mbps 150 ft (45.7 m) at 5.5 Mbps 100 ft (30.5 m) at 11 Mbps</p> <p><b>Note</b> These numbers assume the use of a snap-on antenna with the LM card.</p>
350 series adapters	<p><b>Outdoor</b> 2,000 ft (609.6 m) at 1 Mbps 1,500 ft (457.2 m) at 2 Mbps 1,000 ft (304.8 m) at 5.5 Mbps 800 ft (243.8 m) at 11 Mbps</p> <p><b>Indoor</b> 350 ft (106.7 m) at 1 Mbps 250 ft (76.2 m) at 2 Mbps 200 ft (61 m) at 5.5 Mbps 150 ft (45.7 m) at 11 Mbps</p> <p><b>Note</b> These numbers assume the use of a snap-on antenna with the LM card.</p>
<b>Antenna Specifications</b>	
PC card	Integrated diversity antenna
LM card	Two MMCX antenna connectors
PCI client adapter	RP-TNC connector
<b>Power Specifications</b>	
Operational voltage	5.0 V (+ or -0.25 V)
<b>Receive current steady state</b>	
PC card and LM card	Typically 250 mA
PCI client adapter	Typically 350 mA
<b>Transmit current steady state</b>	
340 series PC card and LM card	Typically 350 mA at 15 dBm
340 series PCI client adapter	Typically 450 mA at 15 dBm

**Table A-1** Technical Specifications for the Cisco Aironet Wireless LAN Client Adapters (continued)

350 series PC card and LM card	Typically 450 mA at 20 dBm
350 series PCI client adapter	Typically 550 mA at 20 dBm
<b>Sleep mode steady state</b>	
340 and 350 series PC card and LM card	Typically 15 mA
340 and 350 series PCI client adapter	Typically 115 mA
<b>Safety and Regulatory Compliance</b>	
Safety	Designed to meet: <ul style="list-style-type: none"> <li>• UL 1950 Third Ed.</li> <li>• CSA 22.2 No. 950-95</li> <li>• IEC 60950 Second Ed., including Amendments 1-4 with all deviations</li> <li>• EN 60950 Second Ed., including Amendments 1-4</li> </ul>
EMI and susceptibility	FCC Part 15.107 & 15.109 Class B ICES-003 Class B (Canada) EN 55022 B AS/NZS 3548 Class B VCCI Class B EN 55024
Radio approvals	FCC Part 15.247 Canada RSS-139-1, RSS-210 Japan Telec 33A EN 300.328
RF exposure	OET-65C RSS-102 ANSI C95.1





## Channels, Power Levels, Antenna Gains

---

This appendix lists the channels supported by the world's regulatory domains. The appendix also lists the maximum power levels and antenna gains for each regulatory domain.

The following topics are covered in this appendix:

- Channel Sets, page B-2
- Maximum Power Levels and Antenna Gains, page B-3

# Channel Sets

The channel identifiers, channel center frequencies, and regulatory domains of each 802.11b 22-MHz-wide channel are shown in Table B-1.

**Table B-1 Channels**

Channel Identifier	Frequency	Regulatory Domains				
		Americas (-A)	ETSI (-E)	Israel (-I)	China (-C)	Japan (-J)
1	2412 MHz	X	X	-	X	X
2	2417 MHz	X	X	-	X	X
3	2422 MHz	X	X	X	X	X
4	2427 MHz	X	X	X	X	X
5	2432 MHz	X	X	X	X	X
6	2437 MHz	X	X	X	X	X
7	2442 MHz	X	X	X	X	X
8	2447 MHz	X	X	X	X	X
9	2452 MHz	X	X	X	X	X
10	2457 MHz	X	X	-	X	X
11	2462 MHz	X	X	-	X	X
12	2467 MHz	-	X	-		X
13	2472 MHz	-	X	-		X
14	2484 MHz	-	-	-		X



**Note**

Mexico is included in the Americas regulatory domain; however, only channels 9 through 11 can be used in Mexico. Users are responsible for ensuring that the channel set configuration is in compliance with the regulatory standards of Mexico.



**Note**

France is included in the ETSI regulatory domain; however, only channels 10 through 13 can be used in France. Users are responsible for ensuring that the channel set configuration is in compliance with the regulatory standards of France.



# Maximum Power Levels and Antenna Gains

An improper combination of power level and antenna gain can result in equivalent isotropic radiated power (EIRP) above the amount allowed per regulatory domain. Table B-2 indicates the maximum power levels and antenna gains allowed for each regulatory domain.

**Table B-2 Maximum Power Levels Per Antenna Gain**

Regulatory Domain	Antenna Gain (dBi)	Maximum Power Level (mW)
Americas (-A) (4 watts EIRP maximum)	0	100
	2.2	100
	5.2	100
	6	100
	8.5	100
	12	100
	13.5	100
	21	20
ETSI (-E) (100 mW EIRP maximum)	0	100
	2.2	50
	5.2	30
	6	30
	8.5	5
	12	5
	13.5	5
	21	1
Israel (-I) (100 mW EIRP maximum)	0	100
	2.2	50
	5.2	30
	6	30
	8.5	5
	12	5
	13.5	5
	21	1

Table B-2 Maximum Power Levels Per Antenna Gain (continued)

Regulatory Domain	Antenna Gain (dBi)	Maximum Power Level (mW)
China (-C) (10 mW EIRP maximum)	0	5
	2.2	5
	5.2	n/a
	6	n/a
	8.5	n/a
	12	n/a
	13.5	n/a
	21	n/a
Japan (-J) (10 mW/MHz EIRP maximum)	0	50
	2.2	30
	5.2	30
	6	30
	8.5	n/a
	12	n/a
	13.5	5
	21	n/a



## Declarations of Conformity and Regulatory Information

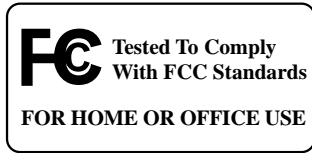
---

This appendix provides declarations of conformity and regulatory information for the Cisco Aironet Wireless LAN Client Adapters.

These topics are covered in this section:

- Manufacturers Federal Communication Commission Declaration of Conformity Statement, page C-2
- Department of Communications – Canada, page C-3
- European Community, Switzerland, Norway, Iceland, and Liechtenstein, page C-4
- Declaration of Conformity for RF Exposure, page C-6
- Guidelines for Operating Cisco Aironet Wireless LAN Client Adapters in Japan, page C-7

# Manufacturers Federal Communication Commission Declaration of Conformity Statement



## Models

AIR-PCM34X, AIR-LMC34X, AIR-PCI34X, AIR-PCM35X, AIR-LMC35X, AIR-PCI35X

## FCC Certification Number

LDK102038 (AIR-PCM34x),  
LDK102035 (AIR-LMC34x and AIR-PCI34x)  
LDK102040 (AIR-xxx35x)

## Manufacturer

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA

This device complies with Part 15 rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits of a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential environment. This equipment generates, uses, and radiates radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference. However, there is no guarantee that interference will not occur. If this equipment does cause interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase separation between the equipment and receiver.
- Connect the equipment to an outlet on a circuit different from which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician.



### Caution

---

The Part 15 radio device operates on a non-interference basis with other devices operating at this frequency. Any changes or modification to said product not expressly approved by Cisco could void the user's authority to operate this device.

---

# Department of Communications – Canada

## Canadian Compliance Statement

This Class B Digital apparatus meets all the requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe B respecte les exigences du Règlement sur le matériel brouilleur du Canada.

This device complies with Class B Limits of Industry Canada. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

The device is certified to the requirements of RSS-139-1 and RSS-210 for 2.4-GHz spread spectrum devices. The use of this device in a system operating either partially or completely outdoors may require the user to obtain a license for the system according to the Canadian regulations. For further information, contact your local Industry Canada office.

## European Community, Switzerland, Norway, Iceland, and Liechtenstein

### Declaration of Conformity with Regard to the R&TTE Directive 1999/5/EC

Deutsch:	Dieses Great entspricht den grundlegenden Anforderungen und den weiteren entsprechenden Vorgaben der Richtlinie 1999/5/EU.
Dansk:	Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Direktiv 1999/5/EF.
English:	This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español:	Este equipo cumple con los requisitos esenciales así como con otras disposiciones de la Directiva 1999/5/CE.
Ελληνικά:	Αυτός ο εξοπλισμός είναι σε συμμόρφωση με τις ουσιαστικές απαιτήσεις και άλλες σχετικές διατάξεις της Οδηγίας 1999/5/EC.
Français:	Cet équipement est conforme aux exigences essentielles et aux autres dispositions pertinentes de la Directive 1999/5/EC.
Íslenska:	Þetta tæki er samkvæmt grunnkröfum og öðrum viðeigandi ákvæðum Tilskipunar 1999/5/EC.
Italiano:	Questo apparato é conforme ai requisiti essenziali ed agli altri principi sanciti dalla Direttiva 1999/5/CE.

50341

Nederlands:	Dit apparaat voldoet aan de essentiële eisen en andere van toepassing zijnde bepalingen van de Richtlijn 1999/5/EC.
Norsk:	Dette utstyret er i samsvar med de grunnleggende krav og andre relevante bestemmelser i EU-direktiv 1999/5/EF.
Português:	Este equipamento está em conformidade com os requisitos essenciais e outras provisões relevantes da Directiva 1999/5/EC.
Suomi:	Tämä laite täyttää direktiivin 1999/5/EY oleelliset vaatimukset ja on siinä asetettujen muiden laitetta koskevien määräysten mukainen.
Svenska:	Denna utrustning är i överensstämmelse med de väsentliga kraven och andra relevanta bestämmelser i Direktiv 1999/5/EC.

50342

The Declaration of Conformity related to this product can be found at this URL:  
<http://www.ciscofax.com>.

For the 340 series, the following standards were applied:

- Radio: ETS 300.328
- EMC: ETS 300.826
- Safety: EN 60950

The following CE mark is affixed to the 340 series equipment:



For the 350 series, the following standards were applied:

- Radio: EN 300.328-1, EN 300.328-2
- EMC: EN 301 489-1, EN 301 489-17
- Safety: EN 60950

The following CE mark is affixed to the 350 series equipment (except for the mini-PCI card):



The above CE mark is required as of April 8, 2000 but might change in the future.

The following CE mark is affixed to the 350 series mini-PCI card:



**Note**

This equipment is intended to be used in all EU and EFTA countries. Outdoor use may be restricted to certain frequencies or may require a license for operation. For more details, contact Cisco Corporate Compliance.



**Note**

Combinations of power levels and antennas resulting in a radiated power level of above 100 mW equivalent isotropic radiated power (EIRP) are considered as not compliant with the above mentioned directive and are not allowed for use within the European community and countries that have adopted the European R&TTE directive 1999/5/EC and the CEPT recommendation Rec 70.03. For more details on legal combinations of power levels and antennas, contact Cisco Corporate Compliance.

## Declaration of Conformity for RF Exposure

The radio module has been evaluated under FCC Bulletin OET 65C and found compliant to the requirements as set forth in CFR 47 Sections 2.1091, 2.1093, and 15.247 (b) (4) addressing RF Exposure from radio frequency devices.



# Guidelines for Operating Cisco Aironet Wireless LAN Client Adapters in Japan

This section provides guidelines for avoiding interference when operating Cisco Aironet Wireless LAN Client Adapters in Japan. These guidelines are provided in both Japanese and English.

## Japanese Translation

この機器の使用周波数帯では、電子レンジ等の産業・科学・医療用機器のほか工場の製造ライン等で使用されている移動体識別用の構内無線局（免許を要する無線局）及び特定小電力無線局（免許を要しない無線局）が運用されています。

- 1 この機器を使用する前に、近くで移動体識別用の構内無線局及び特定小電力無線局が運用されていないことを確認して下さい。
- 2 万一、この機器から移動体識別用の構内無線局に対して電波干渉の事例が発生した場合には、速やかに使用周波数を変更するか又は電波の発射を停止した上、下記連絡先にご連絡頂き、混信回避のための処置等(例えば、パーティションの設置など)についてご相談して下さい。
- 3 その他、この機器から移動体識別用の特定小電力無線局に対して電波干渉の事例が発生した場合など何かお困りのことが起きたときは、次の連絡先へお問い合わせ下さい。

連絡先 : 03-5219-6000

43768

## English Translation

This equipment operates in the same frequency bandwidth as industrial, scientific, and medical devices such as microwave ovens and mobile object identification (RF-ID) systems (licensed premises radio stations and unlicensed specified low-power radio stations) used in factory production lines.

1. Before using this equipment, make sure that no premises radio stations or specified low-power radio stations of RF-ID are used in the vicinity.
2. If this equipment causes RF interference to a premises radio station of RF-ID, promptly change the frequency or stop using the device; call the contact number and ask for recommendations on avoiding radio interference, such as setting partitions.
3. If this equipment causes RF interference to a specified low-power radio station of RF-ID, call the contact number.

Contact Number: 03-5219-6000





## Translated Safety Warnings

---

This appendix provides translations of the safety warnings that appear in this publication. These translated warnings apply to other documents in which they appear in English.

These topics are covered in this section:

- Explosive Device Proximity Warning, page D-2
- Lightning Activity Warning, page D-3
- Installation Warning, page D-3
- Circuit Breaker (15A) Warning, page D-4

# Explosive Device Proximity Warning



## Warning

Do not operate your wireless network device near unshielded blasting caps or in an explosive environment unless the device has been modified to be especially qualified for such use.

## Waarschuwing

Gebruik dit draadloos netwerkapparaat alleen in de buurt van onbeschermd ontstekers of in een omgeving met explosieven indien het apparaat speciaal is aangepast om aan de eisen voor een dergelijk gebruik te voldoen.

## Varoitus

Älä käytä johdotonta verkkolaitetta suojaamattomien räjäytysnallien läheisyydessä tai räjäytysalueella, jos laitetta ei ole erityisesti muunnettu sopivaksi sellaiseen käyttöön.

## Attention

Ne jamais utiliser un équipement de réseau sans fil à proximité d'un détonateur non blindé ou dans un lieu présentant des risques d'explosion, sauf si l'équipement a été modifié à cet effet.

## Warnung

Benutzen Sie Ihr drahtloses Netzwerkgerät nicht in der Nähe ungeschützter Sprengkapseln oder anderer explosiver Stoffe, es sei denn, Ihr Gerät wurde eigens für diesen Gebrauch modifiziert und bestimmt.

## Avvertenza

Non utilizzare la periferica di rete senza fili in prossimità di un detonatore non protetto o di esplosivi a meno che la periferica non sia stata modificata a tale proposito.

## Advarsel

Ikke bruk den trådløse nettverksenheten nært inntil uisolerte fenghetter eller i et eksplosivt miljø med mindre enheten er modifisert slik at den tåler slik bruk.

## Aviso

Não opere o dispositivo de rede sem fios perto de cápsulas explosivas não protegidas ou num ambiente explosivo, a não ser que o dispositivo tenha sido modificado para se qualificar especialmente para essa utilização.

## ¡Advertencia!

No utilizar un aparato de la red sin cable cerca de un detonador que no esté protegido ni tampoco en un entorno explosivo a menos que el aparato haya sido modificado con ese fin.

## Varning!

Använd inte den trådlösa nätverksenheten i närheten av oskyddade tändhattar eller i en explosiv miljö om inte enheten modifierats för att kunna användas i sådana sammanhang.

## Lightning Activity Warning




---

<b>Warning</b>	Do not work on the system or connect or disconnect cables during periods of lightning activity.
<b>Waarschuwing</b>	Tijdens onweer dat gepaard gaat met bliksem, dient u niet aan het systeem te werken of kabels aan te sluiten of te ontkoppelen.
<b>Varoitus</b>	Älä työskentele järjestelmän parissa äläkä yhdistä tai irrota kaapeleita ukkosilmalla.
<b>Attention</b>	Ne pas travailler sur le système ni brancher ou débrancher les câbles pendant un orage.
<b>Warnung</b>	Arbeiten Sie nicht am System und schließen Sie keine Kabel an bzw. trennen Sie keine ab, wenn es gewittert.
<b>Avvertenza</b>	Non lavorare sul sistema o collegare oppure scollegare i cavi durante un temporale con fulmini.
<b>Advarsel</b>	Utfør aldri arbeid på systemet, eller koble kabler til eller fra systemet når det tordner eller lyner.
<b>Aviso</b>	Não trabalhe no sistema ou ligue e desligue cabos durante períodos de mau tempo (trovoada).
<b>¡Advertencia!</b>	No operar el sistema ni conectar o desconectar cables durante el transcurso de descargas eléctricas en la atmósfera.
<b>Varning!</b>	Vid åska skall du aldrig utföra arbete på systemet eller ansluta eller koppla loss kablar.

---

## Installation Warning




---

<b>Warning</b>	Read the installation instructions before you connect the system to its power source.
<b>Waarschuwing</b>	Raadpleeg de installatie-aanwijzingen voordat u het systeem met de voeding verbindt.
<b>Varoitus</b>	Lue asennusohjeet ennen järjestelmän yhdistämistä virtalähteeseen.

Attention	Avant de brancher le système sur la source d'alimentation, consulter les directives d'installation.
Warnung	Lesen Sie die Installationsanweisungen, bevor Sie das System an die Stromquelle anschließen.
Avvertenza	Consultare le istruzioni di installazione prima di collegare il sistema all'alimentatore.
Advarsel	Les installasjonsinstruksjonene før systemet kobles til strømkilden.
Aviso	Leia as instruções de instalação antes de ligar o sistema à sua fonte de energia.
¡Advertencia!	Ver las instrucciones de instalación antes de conectar el sistema a la red de alimentación.
Varning!	Läs installationsanvisningarna innan du kopplar systemet till dess strömförsörjningsenhet.

## Circuit Breaker (15A) Warning



### Warning

This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15A U.S. (240 VAC, 10A international) is used on the phase conductors (all current-carrying conductors).

### Waarschuwing

Dit produkt is afhankelijk van de installatie van het gebouw voor kortsluit- (overstroom)beveiliging. Controleer of er een zekering of stroomverbreker van niet meer dan 120 Volt wisselstroom, 15 A voor de V.S. (240 Volt wisselstroom, 10 A internationaal) gebruikt wordt op de fasegeleiders (alle geleiders die stroom voeren).

### Varoitus

Tämä tuote on riippuvainen rakennukseen asennetusta oikosulkusuojauksesta (ylivirtasuojauksesta). Varmista, että vaihevirtajohtimissa (kaikissa virroitetuissa johtimissa) käytetään Yhdysvalloissa alle 120 voltin, 15 ampeerin ja muissa muissa maissa 240 voltin, 10 ampeerin sulaketta tai suojakytintä.

### Attention

Pour ce qui est de la protection contre les courts-circuits (surtension), ce produit dépend de l'installation électrique du local. Vérifier qu'un fusible ou qu'un disjoncteur de 120 V alt., 15 A U.S. maximum (240 V alt., 10 A international) est utilisé sur les conducteurs de phase (conducteurs de charge).

Warnung	Dieses Produkt ist darauf angewiesen, daß im Gebäude ein Kurzschluß- bzw. Überstromschutz installiert ist. Stellen Sie sicher, daß eine Sicherung oder ein Unterbrecher von nicht mehr als 240 V Wechselstrom, 10 A (bzw. in den USA 120 V Wechselstrom, 15 A) an den Phasenleitern (allen stromführenden Leitern) verwendet wird.
Avvertenza	Questo prodotto dipende dall'installazione dell'edificio per quanto riguarda la protezione contro cortocircuiti (sovracorrente). Verificare che un fusibile o interruttore automatico, non superiore a 120 VCA, 15 A U.S. (240 VCA, 10 A internazionale) sia stato usato nei fili di fase (tutti i conduttori portatori di corrente).
Advarsel	Dette produktet er avhengig av bygningens installasjoner av kortslutningsbeskyttelse (overstrøm). Kontroller at det brukes en sikring eller strømbryter som ikke er større enn 120 VAC, 15 A (USA) (240 VAC, 10 A internasjonalt) på faselederne (alle strømførende ledere).
Aviso	Este produto depende das instalações existentes para protecção contra curto-circuito (sobrecarga). Assegure-se de que um fusível ou disjuntor não superior a 240 VAC, 10A é utilizado nos condutores de fase (todos os condutores de transporte de corrente).
¡Advertencia!	Este equipo utiliza el sistema de protección contra cortocircuitos (o sobrecorrientes) del propio edificio. Asegurarse de que se utiliza un fusible o interruptor automático de no más de 240 voltios en corriente alterna (VAC), 10 amperios del estándar internacional (120 VAC, 15 amperios del estándar USA) en los hilos de fase (todos aquellos portadores de corriente).
Varning!	Denna produkt är beroende av i byggnaden installerat kortslutningsskydd (överströmsskydd). Kontrollera att säkring eller överspänningsskydd används på fasledarna (samtliga strömförande ledare) för internationellt bruk max. 240 V växelström, 10 A (i USA max. 120 V växelström, 15 A).

■ Circuit Breaker (15A) Warning





---

## A

- ad hoc variables 3-16
- antenna
  - attaching 2-4
  - detaching 2-5
  - gains B-3 to B-4
- antennas
  - safety guidelines for 2-2
  - specifications A-4
  - used with client adapters 1-4
- audience vi
- AWCALLID.EXE 4-7, 4-8
- AWCLEAP.EXE 4-6

---

## B

- basic system parameters 3-7

---

## C

- Canadian compliance statement C-3
- channels B-2
- configuration utilities 4-3
- coverage options 1-9
  - heavy overlap 1-9
  - minimal overlap 1-9
  - multiple overlapping systems 1-10

---

## D

- data rates A-3
- data transparency and protocols 1-5

- protocols supported 1-5
- diagnostic utilities 4-4
- dipole antenna 1-4
- diversity antenna 1-4
- documentation
  - feedback viii
  - obtaining vii
  - ordering viii
- documentation CD-ROM vii
- DOS utilities 4-3
  - AWCALLID.EXE 4-7, 4-8
  - AWCLEAP.EXE 4-6
  - getting help in 4-5
  - layout and format 4-4
  - PCMCIA.COM 4-10
  - RADINFO.EXE 4-11
  - running 4-5
  - WEPDOS.EXE 4-9
- driver
  - keywords and settings 3-6
  - overview of 3-2

---

## E

- EIRP, maximum B-3 to B-4

---

## F

- FCC
  - declaration of conformity statement C-2
- firmware
  - loading new versions 4-3
- fragmentation variables 3-9

frequencies B-2

---

infrastructure parameters 3-13

installing hardware 2-1 to 2-8

installing software 3-1 to 3-17

    adapter keywords 3-16

    additional requirements and features 3-5

    ad hoc variables 3-16

    basic system parameters 3-7

    driver keywords and settings 3-6

    fragmentation variables 3-9

    infrastructure parameters 3-13

    network performance variables 3-8

    power management variables 3-10

    scanning variables 3-12

---

## K

keywords

    adapter 3-16

---

## L

LEDs 1-4

    interpreting 5-2

link test 1-5, 4-2

    using Windows 3.xx or MS-DOS to perform 4-2

LM card client adapter

    antenna 1-4

---

## N

NDIS2 driver

    MS-DOS installation 3-3

    Windows for Workgroups installation 3-3

network performance variables 3-8

---

## O

ODI driver

    installation 3-5

overview 1-1 to 1-10

---

## P

package contents 2-3

packet driver

    MS-DOS installation 3-4

PC card client adapter

    antenna 1-4

    removing 2-7

PCMCIA.COM 4-10

power level

    maximum B-3 to B-4

power management variables 3-10

---

## R

RADINFO.EXE 4-11

radio

    compliance specifications A-5

    description 1-3

    regulatory information C-1 to C-7

    specifications A-2 to A-4

regulatory

    domains B-2

related publications vii

RF exposure declaration of conformity statement C-6

---

## S

safety information

    FCC safety compliance statement 2-2

    guidelines 2-2

    specifications A-5

- warnings 2-2
- safety warnings, translated D-1 to D-5
- scanning variables 3-12
- security features 1-6
- sensitivity A-3
- site survey 4-2
- specifications A-2 to A-5
- spread spectrum 1-3
- system configurations 1-6
  - ad hoc wireless LAN 1-6
  - extended infrastructure using repeaters 1-8
  - wireless infrastructure 1-7
  - wireless infrastructure with workstations accessing wired LAN 1-7
- introduction to 1-2
- link test 1-5
- parts of 1-3
- radio ranges 1-4
- removing from computing device 2-7 to 2-8
- security features 1-6
- terminology used 1-3
- unpacking 2-3
- workstations
  - defined 1-3
- World Wide Web vii
  - Cisco.com viii

---

## T

- technical assistance
  - contacting TAC ix
  - obtaining viii
- Technical Assistance Center (TAC) ix
- technical specifications A-2 to A-5
- throughput 3-10
- troubleshooting information
  - location on Cisco.com 5-2

---

## U

- unpacking the client adapter 2-3
- utilities 4-1 to 4-11
  - site survey and link test 4-2

---

## W

- warnings 2-2
- WEPDOS.EXE 4-9
- wireless LAN adapter
  - antenna connectors 2-4
  - inserting into computing device 2-5 to 2-7

